BDO 25 GODINA

NOVEMBAR 2018
NOVEMBER 2018
www.bdo.co.rs

LEGAL HIGHLIGHTS

NOVI ZAKON O ZAŠTITI PODATAKA O LIČNOSTI

I UVOD

Narodna Skupština Republike Srbije je na sednici održanoj 13. novembra 2018. godine usvojila novi Zakon o zaštiti podataka o ličnosti.

Zakon o zaštiti podataka o ličnosti je objavljen u „*Službenom glasniku RS" br. 87/2018* dana 13.11.2018. godine (u daljem tekstu: Zakon) i stupio je na snagu osmog dana od dana objavljivanja, odnosno dana 21.11.2018. godine, s tim da Zakon ima odloženu primenu i **primenjuje se** u roku od devet meseci od dana stupanja na snagu, što je dan **20.08.2019. godine**.

Odložena primena Zakona **se jedino ne odnosi na član 98. Zakona**, kojim je definisano da sa danom stupanja na snagu ovog Zakona prestaje da se vodi Centralni registar zbirki podataka koji je bio uspostavljen prema odredbama prethodnog Zakona o zaštiti podataka o ličnosti, a sa podacima sadržanim u Centralnom registru se postupa u skladu sa propisima kojima se uređuje arhivska građa.

II PRAVNI OSNOV I RAZLOZI DONOŠENJA ZAKONA

Osnov za donošenje Zakona je sadržan u odredbi člana 42. Ustava Republike Srbije kojim je predviđeno da je zaštita podataka o ličnosti zajamčena (stav 1 navedenog člana), da je prikupljanje, držanje, obrada i korišćenje podataka o ličnosti uređuje posebnim zakonom (stav 2 navedenog člana), kao i da svako ima pravo da bude obavešten o prikupljenim podacima o svojoj ličnosti (stav 4 navedenog člana).

Razlozi za donošenje Zakona su brojni. Sa jedne strane je potreba za dopunom prethodnog Zakona o zaštiti podataka o ličnosti sa stanovišta unutrašnjeg prava Republike Srbije i uvođenje zaštite podataka o ličnosti u svim oblastima. Drugi razlog je obaveza Republike Srbije, a u okviru započetog procesa pridruživanja Evropskoj uniji, da uskladi svoje

NEW LAW ON PERSONAL DATA PROTECTION

I INTRODUCTION

The National Assembly of the Republic of Serbia adopted a new Law on Personal Data Protection at its session held on 13 November 2018.

The Law on Personal Data Protection was published in the *Official Gazette of the Republic of Serbia No. 87/2018* on 13 November 2018 (hereinafter: the Law) and came into force on the eighth day from the day of its publication, i.e. on 21 November 2018, provided that the Law has delayed implementation and will be implemented upon expiry of nine months from the date of entry into force which is on 20 August 2019.

The delayed implementation of the Law does not apply only to Article 98 of the Law, which stipulates that as of the date of entry into force of the Law the Central Registry of Databases that was established pursuant to the provisions of the previous Law on Personal Data Protection is not going to be kept any longer, and the data contained in the Central Registry shall be handled in accordance with the regulations governing archival materials.

II LEGAL BASIS AND REASONS FOR THE ADOPTION OF THE LAW

The basis for adoption of the Law is contained in a provision of Article 42 of the Constitution of the Republic of Serbia which stipulates that protection of personal data shall be guaranteed (paragraph 1 of the above-mentioned article), that collecting, keeping, processing and using of personal data shall be regulated by the law (paragraph 2 of the above-mentioned article), as well as that everyone shall have the right to be informed about personal data collected about him/her (paragraph 4 of the above-mentioned article).

The reasons for the adoption of the Law are numerous. On one side, there is a need of supplementing the previous Law on Personal Data Protection from the standpoint of internal law of the Republic of Serbia and introduction of personal data protection in all areas. The other reason is the obligation of the Republic of Serbia, arising from the

nacionalno zakonodavstvo sa važećim propisima Evropske unije.

Konkretan propis Evropske unije je Uredba 2016/679 Evropskog parlamenta i Saveta o zaštiti pojedinca, kao i Direktiva 2016/680 o zaštiti pojedinca u vezi sa obradom njegovih ličnih podataka od strane nadležnih organa.

III PRIMENA ZAKONA

Zakon **se primenjuje** na obradu podataka o ličnosti koja se vrši na automatizovan način, kao i na neautomatizovanu obradu podataka o ličnosti koji čine deo zbirke podataka ili su namenjeni zbirci podataka.

Zakon se **ne primenjuje** na obradu podataka o ličnosti koju vrši fizičko lice za lične potrebe ili potrebe svog domaćinstva.

Zakon **se primenjuje** na obradu podataka o ličnosti koju vrši rukovalac, odnosno obrađivač koji ima sedište, boravište ili prebivalište na teritoriji Republike Srbije, u okviru aktivnosti koje se vrše na teritoriji Republike Srbije.

Zakon **se primenjuje** na obradu podataka o ličnosti lica na koje se podaci odnose koje ima prebivalište, odnosno boravište na teritoriji Republike Srbije, ukoliko se radnje obrade odnose na:

- ponudu robe, odnosno usluge licu na koga se podaci odnose na teritoriji Republike Srbije;
- praćenje aktivnosti lica na koje se podaci odnose, ako se aktivnosti vrše na teritoriji Republike Srbije.

IV IZRAZI I POJMOVI U ZAKONU

Zakon već u uvodnim odredbama u delu značenja izraza, uvodi nove izraze i pojmove u odnosu na prethodni Zakon o zaštiti podataka o ličnosti.

Osnovni pojmovi, a koje je i prethodni Zakon o zaštiti podataka definisao, su:

initiated process of accession to the European Union, to harmonise the national regulations with the effective regulations of the European Union.

The specific regulation of the European Union is the Regulation 2016/679 of the European Parliament and of the Council ("GDPR") on the protection of natural persons regarding processing their personal data by the competent authorities.

III APPLICATION OF THE LAW

The Law **applies** to the processing of personal data performed by automated means, as well as to manual processing of personal data contained or intended to be contained in a database.

The Law **is not applicable** to personal data processing performed by natural persons for personal needs or for the needs of their household.

The Law **is applicable** to processing of the personal data performed by a controller or a processor having a seat, temporary residence or permanent residence on the territory of the Republic of Serbia, within the activities carried out on the territory of the Republic of Serbia.

The Law **applies** to processing of personal data of natural persons to whom the data relate, having permanent or temporary residence in the territory of the Republic of Serbia, if the processing actions relate to the following:

- offering goods or services to the natural persons to whom the data relate in the territory of the Republic of Serbia;
- monitoring the activities of the natural persons to whom the data relate, if the activities are carried out in the territory of the republic of Serbia.

IV TERMS AND CONCEPTS IN THE LAW

The Law introduces new terms and concepts in relation to the previous Law on Personal data Protection already in the introductory provisions in the part related to definitions of terms.

Basic concepts, defined also by the previous Law on Personal data Protection, are the following:

- **Podatak o ličnosti** je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime I identifikacioni broj i dr;
- **Lice na koje se podaci odnose** je fizičko lice čiji se podaci o ličnosti obrađuju;
- **Obrada podataka o ličnosti** je svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima kao što su: prikupljanje, beleženje, razvrstavanje, grupisanje, struktuiranje, pohranjivanje, upodobljavanje, menjanje, otkrivanje, uvid, upotreba, otkrivanje prenosom, odnosno dostavljanjem, umnožavanje, širenje ili na drugi način činjenje dostupnim, upoređivanje, ograničavanje, brisanje ili uništavanje;
- **Zbirka podataka** je svaki strukturisani skup podataka o ličnosti koji je dostupan u skladu sa posebnim kriterijumima;
- **Rukovalac** je fizičko ili pravno lice, kao i organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade.
- **Obrađivač** je fizičko ili pravno lice, kao i organ vlasti koji obrađuje podatke o ličnosti u ime rukovaoca.

- **Personal data** are any data relating to a natural person the identity of whom is determined or determinable, directly or indirectly, especially on the basis of an identity mark, such as name and identification number, etc.;
- **The data subject** is a natural person whose personal data are processed;
- **Personal Data Processing** is any action or a set of actions perfomed by automated means or manually upon the personal data or sets of personal data, such as: collecting, recording, classification, grouping, structuring, storing, adaptation, alteration, disclosure, making available for insight, use, revealing by transmission or delivering, copying, dissemination or otherwise making available, comparing, limiting, deleting or destroying;
- **Personal data filing system** is every structured set of personal data available in accordance with the special criteria;
- **Personal data filing system controller** is a natural person or legal entity or authority determining, individually or jointly with others, the purpose and the manner of personal data processing.
- **The processor** is a natural person or legal entity or authority processing the personal data on behalf of the controller.

Novouvedeni pojmovi u Zakonu su:

- **Pristanak** lica na koje se podaci odnose predstavlja svako dobrovoljno, određeno, informisano I nedvosmisleno izražavanje volje tog lica, kojim to lice, izjavom ili potvrdnom radnjom, daje pristanak za obradu podataka o ličnosti
- **Profilisanje** je svaki oblik automatizovane obrade koji se koristi da bi se ocenilo određeno svojstvo ličnosti (analiza radnog učinka, ekonomskog položaja, zdravstvenog stanja, ličnih okolnosti, interesa, pouzdanosti, ponašanja lokacije ili kretanja);

The newly introduced concepts in the Law are:

- **Consent** of the natural person to whom the data relate is any freely given, specific, informed and unambiguous indication of that person's will, by which the person gives consent on personal data processing by means of a statement or an affirmative action
- **Profiling** is any form of processing by automated means used to evaluate specific personality trait (performance analysis, economic status, health status, personal circumstances, interests, reliability, behavour, location or movement);

- **Pseudonimizacija** je obrada na način koji onemogućava pripisivanje podataka o ličnosti određenom licu bez korišćenja dodatnih podataka, pod uslovom da se ovi podaci čuvaju posebno i da su preduzete tehničke, organizacione i kadrovske mere koje obezbeđuju da se podatak o ličnosti ne može prepisati određenom licu;

- **Povreda podataka o ličnosti** je povreda bezbednosti podataka o ličnosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa podacima o ličnosti koji su preneseni, pohranjeni ili obrađivani;
- **Genetski podatak** je podatak o ličnosti koji se odnosi na nasleđena ili strečena genetska obeležja fizičkog lica koja pružaju jedinstvenu informaciju o fiziologiji ili zdravlju tog lica, a naročito oni koji su dobijeni analizom iz uzorka biološkog porekla;
- **Biometrijski podatak** je podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa fizičkim obeležjima, fiziološkim obeležjima ili obeležjima ponašanja fizičkog lica, koja omogućava ili potvrđuje jedinstvenu identifikaciju tog lica (slika njegovog lica ili njegovi daktiloskopski podaci).

- **Pseudonymisation** is a personal data processing in a way that prevents the attribution of personal data to a specific person without the use of additional data, provided that these data are stored separately and that technical, organisational and personnel measures have been taken which ensure that the personal data cannot be attributed to a specific person;
- **Personal data breach** is a violation of personal data safety leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data which are transmitted, stored or processed;
- **Genetic data** are personal data relating to inherited or acquired genetic characteristics of a natural person which provide the unique information on physiology or health of that person, and in particular those obtained by analysis from a sample of biological origin;

- **Biometric data** are personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person (facial images or dactyloscopic data);

V NAČELA OBRADE

Zakon prepoznaje osnovna načela prilikom obrade podataka o ličnosti i to:

1) podaci se moraju obrađivati **zakonito, pošteno i transparentno** u odnosu na lice čiji se podaci obrađuju;
2) podaci se prikupljaju **u svrhe** koje su konkretno **određene, izričite, opravdane i zakonite** i ne mogu se obrađivati u druge svrhe;
3) podaci moraju biti **primereni, bitni i ograničeni** na ono što je neophodno u odnosu na svrhu obrade;
4) podaci moraju biti **tačni i** ukoliko je neophodno **ažurirani**;

V PRINCIPLES OF PROCESSING

The Law recognises the basic principles when processing personal data as follows:

1) The processing of personal data should be **lawful, fair and transparent** to the data subject;
2) The data are collected for the **purposes** that are particularly **specified, explicit, justified and legitimate** and cannot be processed for other purposes;
3) The data should be **adequate, relevant and limited** to what is necessary for the purposes for which they are processed;
4) The data should be **accurate** and, where necessary, **kept up to date**;

5) podaci se moraju čuvati u obliku koji omogućava identifikaciju lica **samo u roku koji je neophodan** za ostvarivanje svrhe obrade;

6) podaci se moraju obrađivati na način koji **obezbeđuje** odgovarajuću **zaštitu podataka o ličnosti,** uključujući i **zaštitu od neovlašćene ili nezakonite obrade**, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera.

Za primenu svih navedenih načela odgovoran je rukovalac i u slučaju potrebe dužan je da predoči njihovu primenu.

VI ZAKONITOST OBRADE

Uslov da bi obrada podataka o ličnosti bila zakonita je:

1) da je lice na koje se podaci odnose **dalo pristanak** na obradu svojih podataka;
2) da je obrada **neophodna radi izvršenja ugovora** zaključenog sa licem na koje se podaci odnose;
3) da je obrada **neophodna radi poštovanja pravnih obaveza rukovaoca**;

4) da je obrada **neophodna radi zaštite životno važnih interesa** lica na koje se podaci odnose;
5) da je obrada **neophodna u cilju obavljanja poslova u javnom interesu** ili radi izvršenja zakonom propisanih ovlašćenja rukovaoca;

6) da je obrada **neophodna u cilju ostvarivanja legitimnih interesa** rukovaoca ili treće strane.

VII PRISTANAK LICA

Ukoliko se obrada podataka o licu **zasniva na pristanku**, a ne na drugom osnovu obrade podataka, rukovalac **mora da poseduje dokaz** o pristanku lica čiji se podaci obrađuju.

Pristanak mora biti **jednostavan, razumljiv i lako dostupan**, a lice koje daje pristanak pre davanja

5) The data should be kept in a form which permits identification of the natural persons **for no longer than is necessary** for the purposes for which the personal data are processed;
6) The data should be processed in a manner that ensures appropriate **security of the personal data**, including **protection against unauthorised or unlawful processing** and against accidental loss, destruction or damage, using appropriate technical, organisational or personnel measures.

The controller is responsible for compliance with all the above principles and obliged, if necessary, to adduce their application.

VI LAWFULNESS OF PROCESSING

Processing shall be lawful only if and to the extent that the following applies:

1) The data subject **has given consent** to the processing of his or her personal data;
2) processing is **necessary for the performance of a contract** to which the data subject is party;
3) processing is **necessary for compliance with a legal obligation to which the controller is subject**;
4) processing is **necessary in order to protect the vital interests** of the data subject;

5) processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
6) processing is **necessary for the purposes of the legitimate interests** pursued by the controller or by a third party.

VII CONSENT OF DATA SUBJECTS

Where the processing of the personal data is **based on consent**, and not on another basis of data processing, the controller **shall own an evidence** of the consent of the data subject.

The consent shall be in **simple, intelligible and easily accessible form**, and, prior to expressing his

pristanka mora biti upoznato da pristanak može da opozove.

Lice na koga se podaci odnose i koje je dalo pristanak **ima pravo da u svakom trenutku opozove** svoj pristanak.

VIII INFORMACIJE I PRISTUP PODACIMA

Rukovalac je dužan da licu na koje se podaci odnose pruži informacije definisane odredbama Zakona, kao i da omogući pristup tim podacima.

Informacije koje je dužan da pruži su sledeće:

1) informacije o identitetu i kontakt podacima rukovaoca, kao i njegovog predstavnika ako je određen;
2) kontakt podatke lica za zaštitu podataka o ličnosti;
3) o svrsi obrade i pravnom osnovu obrade;
4) o postojanju legitimnog interesa rukovaoca ili treće strane;
5) informacije o primaocu ukoliko postoji;
6) o nameri rukovaoca, ukoliko postoji, da podatke o ličnosti iznese u drugu državu ili međunarodnu orhganizaciju.

Pored navedenih informacija rukovalac je dužan da licu pruži i sledeće dodatne informacije:

1) o roku čuvanja podataka o ličnosti i kriterijumima za njihovo prikupljanje;
2) o postojanju prava lica da od rukovaoca zahteva pristup, ispravku ili brisanje svojih podataka;
3) o postojanju prava na ograničenje obrade, na prigovor, kao i na prenosivost podataka;
4) o postojanju prava na opoziv pristanka u bilo koje vreme;
5) o pravu da se podnese pritužba Povereniku;

or her consent, the data subject shall be informed about having the right to withdraw the consent.

The data subject who has consented to processing of personal data shall have the **right to withdraw his or her consent at any time**.

VIII INFORMATION AND ACCESS TO THE DATA

The controller shall provide the data subject with information defined by the provisions of the Law, as well as with the access to the information.

The controller shall provide the data subject with all of the following information:

1) the identity and the contact details of the controller and, where applicable, of the controller's representative;
2) the contact details of the data protection officer;
3) the purposes of as well as the legal basis for the processing;
4) the existence of the legitimate interests pursued by the controller or by a third party;
5) the recipients of the personal data, if any;
6) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.

In addition to the above information the controller shall provide the data subject with the following further information:

1) the period for which the personal data will be stored and the criteria used for their collection;
2) the existence of the right to request from the controller access to and rectification or erasure of personal data;
3) the existence of the right to request from the controller restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
4) the existence of the right to withdraw consent at any time;
5) the right to lodge a complaint with the Commisioner;

6) o osnovu davanja podataka o ličnosti: da li je u pitanju zakonska ili ugovorna obaveza ili neophodan uslov za zaključenje ugovora, kao i o obavezi da lice da podatke koji se na njega odnose i o posledicama ako ne da podatke;

7) o postojanju automatizovanog donošenja odluke.

Lice čiji se podaci obrađuju ima pravo da od rukovaoca zahteva pristup tim podacima, kao i kopiju podataka koje rukovalac obrađuje.

6) regarding the basis of provision of personal data: whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
7) the existence of automated decision-making.

The data subject has the right to request from the controller the right to access the data, as well as copy of the data that is processed by the controller.

IX OBAVEZE RUKOVAOCA

Zakon daje samo opšte definicije obaveza rukovaoca, bez ulaženja u njihovo preciziranje.

Prema odredbi člana 41. Zakona rukovalac je dužan da preduzme odgovarajuće tehničke, organizacione i kadrovske mere kako bi omogućio da se obrada podataka o ličnosti vrši na zakonit način.

Pod merama se smatra i donošenje internih akata o zaštiti podataka o ličnosti.

IX RESPONSIBILITY OF THE CONTROLLER

The Law provides general definitions of the controller's responsibilities only, without details thereof.

Pursuant to a provision of Article 41 of the Law the controller shall implement appropriate technical, organisational and personnel measures to ensure that personal data processing is performed in compliance with the legislation.

The measures shall also include the implementation of appropriate data protection policies by the controller.

X MERE ZAŠTITE

U okviru tehničkih, organizacionih i kadrovskih mera zaštite rukovalac i obrađivač su dužni da sprovode sve mere zaštite kako bi dostigli odgovarajući nivo bezbednosti u odnosu na rizik.

Zakon naročito prepoznaje sledeće mere zaštite:

1) pseudonimizacija i kriptozaštita podataka o ličnosti;
2) sposobnost obezbeđivanja trajne poverljivosti, integriteta, raspoloživosti i otpornosti sistema i usluga obrade;

X PROTECTION MEASURES

Within technical, organisational and personnel measures of protection the controller and the processor are obliged to carry out all protection measures in order to achieve adequate level of security in relation to risk.

The Law specifically recognises the following protection measures:

1) Pseudonymization and encryption of personal data;
2) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

3) obezbeđivanje uspostavljanja ponovne raspoloživosti I pristupa podacima o ličnosti u slučaju fizičkih ili tehničkih incidenata u najkraćem roku;
4) postupak redovnog testiranja, ocenjivanja i procenjivanja delotvornosti tehničkih, organizacionih i kadrovskih mera bezbednosti obrade.

Takođe, rukovalac je dužan da obezbedi da se uvek obrađuju samo oni podaci o ličnosti koji su neophodni za ostvarivanje svake pojedinačne svrhe obrade.

XI OBRAĐIVAČ

Ukoliko se obrada vrši u ime rukovaoca, rukovalac može da odredi kao obrađivača samo ono lice ili organ vlasti koji u potpunosti garantuje primenu odgovarajućih tehničkih, organizacionih i kadrovskih mera na način da se vrši uz poštovanje odredaba Zakona.

Obrađivač može poveriti obradu drugom obrađivaču samo ako ga rukovalac za to ovlasti davanjem pismenog ovlašćenja.

Pravni odnos između rukovaoca i obrađivača mora biti uređen ugovorom ili drugim pravno obavezujućim aktom, kojim se definišu osnovni elementi ugovornog odnosa (predmet i trajanje obrade, priroda i svrha obrade, vrsta podataka o ličnosti koja se obrađuje, prava i obaveze obe ugovorne strane i dr.).

Navedenim ugovorom, odnosno drugim pravno obavezujućim aktom se definiše da je obrađivač dužan da:

1) obrađuje podatke o ličnosti isključivo na osnovu pismenih uputstava rukovaoca;
2) obezbedi da se fizičko lice koje je ovlašćeno da obrađuje podatke o ličnosti obavezalo na čuvanje poverljivosti podataka;
3) preduzme sve Zakonom definisane mere bezbednosti prilikom obrade;
4) poštuje Zakonom definisane uslove za poveravanje obrade drugom obrađivaču;

3) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident as soon as possible;
4) a process for regularly testing, assessing and evaluating the effectiveness of technical, organisational and personnel measures for ensuring the security of the processing.

Also, the controller is obliged to ensure that the data processed are only the ones necessary for each of the purposes for which they are processed.

XI THE PROCESSOR

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing full guarantees to implement appropriate technical, organisational and personnel measures in such a manner that will meet the requirements of the Law.

The processor shall not engage another processor without prior written authorisation of the controller.

The legal relationship between the controller and the processor shall be governed by a contract or other legal act defining the basic elements of the contractual relationship (the subject and duration of the processing, the nature and purpose of the processing, the type of personal data being processed, rights and obligations of both contracting parties, etc.).

The above-mentioned contract or other legal act shall stipulate that the processor:

1) processes the personal data only on the basis of documented instructions from the controller;
2) ensures that persons authorised to process the personal data have committed themselves to confidentiality;
3) takes all protection measures defined by the Law during the processing;
4) respects legally defined conditions for for engaging another processor;

5) pomaže rukovaocu primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera prilikom ispunjavanja obaveza rukovaoca u vezi prava lica na koje se podaci odnose (pravo na ispravku, dopunu, brisanje itd);

6) pomaže rukovaocu u ispunjavanju zakonskih obaveza koje se odnose na: obaveštavanja lica na koga se podaci odnose u slučaju povrede njihovih podataka, izvršenje procene uticaja predviđenih radnji obrade na zaštitu podataka o ličnosti, kao i prilikom traženja prethodnog mišljenja od Poverenika u slučaju postojanja visokog rizika za obradu podataka;
7) nakon okončanja ugovorenih radnji obrade rukovaocu vrati sve podatke o ličnosti, odnosno izbriše sve podatke i kopije pidataka;
8) učini sve informacije dostupnim rukovaocu koje su neophodne za predočavanje ispunjenosti obaveza obrađivača.

5) assists the controller in ensuring compliance with the obligations relating to the rights of the data subject (right to rectification, ammendment, erasure, etc.) by applying adequate technical, organisational and personnel measures;
6) assists the controller in ensuring compliance with legal obligations relating to: informing the data subject in case of personal data breach, carrying out an assesment of the impact of the envisaged processing actions to the personal data protection, as well as in requesting prior opinion of the Commisioner in case of occurrence of high level of risk for data processing;
7) returns to the controller all the personal data or erases all the data or copies thereof upon termination of the contracted processing actions;
8) makes the information which necessary for demonstrating the fulfillment of the obligations of processor available to the controller.

XII EVIDENCIJA RADNJI OBRADE

Rukovalac je dužan da vodi evidenciju o radnjama obrade za koje je odgovoran, a koja sadrži informacije o:

1) imenu i kontakt podacima rukovaoca;

2) svrsi obrade;
3) vrsti lica na koje se podaci odnose I vrsti podataka o ličnosti;
4) vrsti primalaca kojima su podaci otkriveni;

5) prenosu podataka u druge države ili međunarodne organizacije;
6) roku čijim istekom se brišu određeni podaci;

7) opštem opisu mera zaštite.

XII RECORDS OF PROCESSING ACTIVITIES

The controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

1) the name and contact details of the controller;
2) the purposes of the processing;
3) the categories of data subjects and of the categories of personal data;
4) the categories of recipients to whom the personal data have been disclosed;
5) transfers of personal data to a third country or an international organisation;
6) the time limits for erasure of the different categories of data;
7) the general description of the security measures.

XIII POVERENIK

Rukovalac, obrađivač i njihovi predstavnici su dužni da sarađuju sa Poverenikom u vršenju njegovih ovlašćenja.

Rukovalac je dužan da Poverenika bez odlaganja, a najkasnije u roku od 72 časa obavesti o povredi podataka o ličnosti koja može da proizvede rizik po prava i slobode fizičkih lica.

Obaveštenje Povereniku mora da sadrži sve informacije definisane Zakonom (opis prirode povrede, kontakt podatke lica za zaštitu podataka o ličnosti, opis mogućih posledica povrede, opis preduzetih mera od strane rukovaoca).

Poverenik svoja ovlašćenja vrši u skladu sa odredbama Zakona, na teritoriji Republike Srbije.

Najvažnija ovlašćenja Poverenika su, između ostalih, sledeća;

1) vrši inspekcijski nadzor i obezbeđuje primenu Zakona;
2) na zahtev lica na koje se podaci odnose, pruža informacije o njihovim pravima koja su propisana Zakonom;
3) postupa po pritužbama lica na koje se podaci odnose i utvrđuje da li je došlo do povrede Zakona;
4) daje pismena mišljenja u pogledu procene uticaja na zaštitu podataka o ličnosti;
5) vodi različte evidencije u skladu sa Zakonom (podaci o licu za zaštitu podataka o ličnosti, povrede Zakona);
6) podstiče izdavanje sertifikata za zaštitu podataka i propisuje i objavljuje kriterijume za akreditaciju sertifikacionog tela.

Poverenik propisuje obrazac pritužbe, koja se može poneti i elektronskim putem.

XIII THE COMMISIONER

The controller, the processor and their representatives shall cooperate with the Commissioner in exercising his powers.

The controller shall without undue delay and not later than 72 hours after having become aware of it, notify the commissioner, on any personal data breach that is likely to result in a risk to the rights and freedoms of natural persons.

The notification for the Commissioner shall contain all information prescribed by the Law (the description of the nature of personal data breach, contact details of the personal data protection officer, description of ther consequences of personal data breach, description of measures taken by the controller).

The commissioner exercises his powers pursuant to provisions of the Law in the territory of the Republic of Serbia.

The most important powers of the Commissioner are, among others, the following:

1) performs inspection and ensures the implementation of the Law;
2) at the request of the data subject, provides information on their rights which are prescribed by the Law;
3) acts on complaints of data subjects and determines whether there has been a violation of the Law;
4) provides in writing the opinions regarding the assessment of impact to personal data protection;
5) keeps various records in accordance with the Law (the data on person authorised for protection of personal data, violations of the Law);
6) encourages issuing of data protection certificates and prescribes and publishes the criteria for accreditation of the certification body.

The Commissioner prescribes the form for complaints, which may also be submitted electronically.

XIV LICE ZA ZAŠTITU PODATAKA O LIČNOSTI

Rukovaocu i obrađivaču Zakonom nije definisana obaveza određivanja lica za zaštitu podataka o ličnosti, osim u sledećim slučajevima kada postoji obaveza njegovog određivanja:

1) kada se obrada vrši od strane organa vlasti;

2) kada se osnovne aktivnosti rukovaoca i obrađivača sastoje u radnjama obrade koje po svojoj prirodi, obimu ili svrsi zahtevaju redovan i sistematizovan nadzor velikog broja lica na koje se podaci odnose;

3) kada se osnovne aktivnosti rukovaoca i obrađivača sastoje u obradi posebnih podataka o ličnosti (etičko ili rasno poreklo, političko mišljenje, versko ili filozofsko uverenje, članstvo u sindikatu, obrada genetskih ili biometrijskih podataka, podaci o zdravstvenom stanju ili seksualnoj orijentaciji lica).

Lice za zaštitu podataka o ličnosti može biti zaposleno kod rukovaoca ili obrađivača ili može obavljati ove poslove po osnovu ugovora.

Rukovalac i obrađivač su dužni da objave kontakt podatke lica za zaštitu podataka o ličnosti i dostave ih Povereniku, koji vodi evidenciju lica za zaštitu podataka o ličnosti.

Takođe, rukovalac i obrađivač su dužni da licu za zaštitu podataka o ličnosti omoguće izvršavanje njegovih obaveza i to:

1) pružanje informacija i davanje mišljenja rukovaocu i obrađivaču o zakonskim obavezama u vezi sa zaštitom podataka o ličnosti;
2) praćenje primene odredbi Zakona i drugih relevantnih propisa u vezi sa zaštitom podataka o ličnosti;
3) davanje mišljenja o proceni uticaja obrade na zaštitu podataka o ličnosti;
4) saradnja sa Poverenikom i savetovanje sa Poverenikom u vezi sa pitanjima koja se odnose na obradu podataka o ličnosti.

XIV DATA PROTECTION OFFICER

The controller and the processor are not obliged by the Law to designate a data protection officer, except in the following cases:

1) where the processing is carried out by a public authority or body;
2) where the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
3) where the core activities of the controller or the processor consist of processing of special categories of data (ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic or biometric data, data on health status or sexual orientation of natural persons).

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

The controller and the processor shall publish the contact details of the data protection officer and communicate them to the Commissioner. The Commissioner keeps record of data protection officers.

Also, the controller and the processor shall enable the data protection officer to perform his/her duties as follows:

1) informing and and advising the controller and the processor of their obligations pursuant to the Law related to personal data protection;
2) monitoring compliance with provisions of this Law and other relevant regulations related to personal data protection;
3) providing advice with regard to assessment of of processing impact to personal data;
4) cooperating with the Commisioner and providing advice to the Commisioner regarding issues relating to personal data processing.

XV OBEZBEĐENJE SERTIFIKATA

Rukovalac i obrađivač mogu da od akreditovanih sertifikacionih tela po sprovedenom postupku i ispunjenju uslova dobiju sertifikat o zaštiti podataka o ličnosti.

Postupak dobijanja sertifikata je dobrovoljan i transparentan.

Sertifikat se po pravilu izdaje na period koji ne može biti duži od tri godine i može se obnavljati ukoliko rukovalac ili obrađivač i dalje ispunjavaju iste propisane uslove i kriterijume za izdavanje sertifikata.

XV CERTIFICATION

The controller and the processor may obtain a certificate of personal data protection from accredited certification bodies upon conducting the procedure and complying with the requirements relating to personal data protection.

The certification shall be voluntary and available via a process that is transparent.

The certificate is usually issued for a maximum period of three years and may be renewed provided that the relevant requirements and criteria continue to be met by the controller or the processor.

XVI PRENOS PODATAKA O LIČNOSTI U DRUGE DRŽAVE I MEĐUNARODNE ORGANIZACIJE

Prenos podataka o ličnosti može se izvršiti od strane rukovaoca ili obrađivača isključivo ukoliko su ispunjeni uslovi propisani Zakonom i to:

1) prenos je neophodno izvršiti u posebne svrhe;
2) prenos se vrši rukovaocu u drugoj državi ili međunarodnoj orgamizacijii ukoliko je u pitanju nadležni organ za obavljanje ovih poslova;
3) prenos se vrši u državu sa liste država koje je odredila Vlada Republike Srbije, a ukoliko to nije slučaj potrebno je primeniti posebne mere zaštite;
4) ukoliko se prenos iz druge države ili međunarodne organizacije vrši u treću državu ili međunarodnu organizaciju, potrebno je da prvi organ prenosa ili drugi nadležni organ da saglasnost na dalji prenos, a pošto je sagledao sve okolnosti od značaja za dalji prenos.

XVI TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Transfers of personal data by the controller or the processor shall take place only if legally prescribed requirements are complied with by the controller and processor such as:

1) the transfer is necessary to be performed for special purposes;
2) the transfer is performed to the controller from third country or international organization if it represents the competent authority for performing such activities;
3) the transfer is performed to a country from the list of countries determined by the Government of the Republic of Serbia, and if this is not the case, special protection measures shall be applied;
4) if the transfer from one third country or international organization is performed to another third country or international organization it is necessary to obtain an approval of further transfer from the first transfer authority or another competent body having considered all the circumstances of importance for the further transfer.

XVII PRAVNA SREDSTVA

Kako je prethodno rečeno lice na koje se podaci odnose ima pravo da podnese pritužbu Povereniku

XVII LEGAL REMEDIES

As stated above, the data subject has the right to file a complaint to the Commissioner if he/she considers

ako smatra da je obrada podataka o njegovoj ličnosti izvršena suprotno Zakonu.

Poverenik je dužan da lice obavesti o toku postupka koji vodi, rezultatima postupka putem donošenja odluke, kao i pravu da pokrene sudski postupak.

Lice na koje se podaci odnose, rukovalac ili obrađivač ili drugo lice na koje se odnosi odluka Poverenika ima pravo da protiv odluke Poverenika putem tužbe pokrene upravni spor u roku od 30 dana od dana prijema odluke.

Takođe, ukoliko Poverenik u roku od 60 dana od dana podnošenja pritužbe od strane lica na koje se podaci odnose ne postupi po pritužbi, lice ima pravo da pokrene upravni spor.

Lice na koje se podaci odnose ima pravo na sudsku zaštitu podnošenjem tužbe nadležnom sudu ako smatra da su mu od strane rukovaoca ili obrađivača povređena prava prilikom obrade njegovih podataka.

XVIII KAZNE ZAPREĆENE ZAKONOM

U slučaju nepostupanja i nepoštovanja odredaba Zakona novčanom kaznom od 50.000 do 2.000.000 dinara će se kazniti rukovalac, odnosno obrađivač sa svojstvom pravnog lica, a odgovorno lice novčanom kaznom od 5.000 do 150.000 dinara.

Novčanom kaznom od 5.000 do 150.000 dinara će se kazniti i fizičko lice koje podatka o ličnosti ne čuva kao profesionalnu tajnu, a koje je saznalo tokom obavljanja svojih poslova.

XIX STUPANJE NA SNAGU

Zakon počinje da se primenjuje po isteku devet meseci od dana stupanja Zakona na snagu, a što je **20.08.2019. godine.**

Početkom primene Zakona prestaje sa primenom Zakon o zaštiti podataka o ličnosti *(„Sl. glasnik RS" br. 97/08, 104/09 – dr. zakon, 68/12-US i 107/12*).

that the processing of his/her personal data is carried out contrary to law.

The Commissioner shall inform the data subject on the course of the conducted procedure, the results of the procedure by means of a decision, as well as of his/her right to initiate court proceedings

The data subject, the controller, the processor or third person to whom the Commissioner's decision is related has the right to initiate an administrative dispute against the Commissioner's decision within 30 days from the date of receipt of the decision.

Also, if the Commissioner does not act on the complaint within 60 days from the date of filing of the complaint by the data subject, the data subject has the right to initiate administrative procedure.

The data subject has a right to judicial protection by filing a lawsuit to the competent court if he deems his rights have been violated by the controller or the processor during the processing.

XVIII FINES PRESCRIBED BY THE LAW

In case of failure to act upon or comply with the provisions of the Law legal entity acting as the controller i.e. the processor shall be punished with the fine of RSD 50.000 to RSD 2.000.000 and the authorised person shall be punished by the fine of RSD 5.000 to RSD 150.000.

A natural person who does not keep as confidential information personal data learned while performing his/her job duties shall be punished by the fine of RSD 5.000 to RSD 150.000.

XIX ENTRY INTO FORCE

The Law shall be implemented upon expiry of nine months from the date of its entry into force which is **on 20 August 2019.**

As of the effective date of this Law, provisions of the Law on Personal Data Protection (*Official Gazette of the Republic of Serbia* No. *97/08, 104/09 – other Law, 68/12-CC and 107/12*) shall become null and void.

Branka Marković
Partner, Tax&Outsourcing
branka.markovic@bdo.co.rs
+381 64 823 23 13

Nataša Sević
Legal Advisor
natasa.sevic@bdo.co.rs
+381 64 823 23 36

Jelena Šegrt Janković
Legal Advisor
jelena.jankovic@bdo.co.rs
+381 64 823 23 52

Knez Mihailova 10
11000 Beograd
+381 11 3281 399
tax@bdo.co.rs

Follow us on:

BDO Tax News SRB | BIH | MNE

GET IT ON Google Play

Download on the App Store

www.bdo.co.rs