ČIJI SU TO NAŠI BROJEVI TELEFONA
WHOSE ARE OUR PHONE NUMBERS

vukmirović mišić law firm
JPM | PARTNER IN MONTENEGRO

JPM | JANKOVIĆ POPOVIĆ MITIĆ

ČIJI SU TO NAŠI BROJEVI TELEFONA/WHOSE ARE OUR PHONE NUMBERS

Publisher: JPM Janković Popović Mitić
Delta House, 8a Vladimira Popovića street
www.jpm.rs
Authors: Ivan Milosevic, Partner and
Alma Karadjuzovic Đinđinović, Senior Associate in Vukmirovic Misic law firm-JPM Partner.
Design and prepress: JPM Janković Popović Mitić

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

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

U Crnoj Gori na snazi je još uvijek Zakon o zaštiti podataka o ličnosti koje je posljednji put mijenjan 03.04.2017. godine ("ZZLP").

U međuvremenu, 25. maja 2018. godine, na snagu je stupila nova Opšta uredba Evropske unije o zaštiti podataka o ličnosti (General Data Protection Regulation – GDPR) ("GDPR"), nov pravni okvir koji određuje način korišćenja podataka o ličnosti građana Evropske unije, kao što su ime, prezime, JMBG, e-mail adresa, broj telefona ali i pristup različitim sajtovima, odnosno podacima koji se ne odnose samo na to ko je osoba, već i na to kako doći do nje.

GDPR bi trebao biti obavezan i za Crnu Goru, s obzirom da sve zakonske akte prilagođavamo aktima u Evropskoj uniji, a sama uredba propisuje i obaveze za pravna i fizička lica koja nisu iz Evropske unije ukoliko online nude robu i usluge rezidentima EU i/ili prate ponašanje rezidenata EU na teritoriji EU.

In Montenegro, the Law on protection of personal data is still in power, and was last amended on April 3, 2017 („LPPI").

In the meantime, on May 25, 2018, the European Union's General Data Protection Regulation („GDPR") entered into power, a new legal frame that determines the manner of using personal data of European Union's citizens, such as the name, surname, Personal ID no, email address, phone number as well as access to different websites, i.e. data not only related to the person itself but also how to identify it.

GDPR should be obligatory for Montenegro, considering our practice of aligning our legal frame with the European Union's, and considering GDPR itself prescribes that legal and natural entities outside of the European Union are subject to the rules of GDPR if they offer goods and services to the residents of European Union and/or monitor the behavior of EU residents within EU territory.

Jedan od ciljeva GDPR jeste da nivo zaštite podataka o ličnosti bude isti na cijeloj teritoriji Evropske unije.

Do danas – usklađivanja ZZLP sa GDPR nije bilo.

Zanimljiva pojava prethodnih dana, pred lokalne izbore u Crnoj Gori koji su se održali dana 23.10.2022. godine, jeste slanje SMS poruka brojnim građanima od strane različitih političkih partija.

Nameće se više pitanja:

1. odakle političkim partijama brojevi telefona građana,
2. da li se krši pravo na privatnost građana,
3. da li je broj telefona lični podatak, te brojna druga.

Današnja napredna tehnologija nam uz pomoć aplikacija koje svakodnevno koristimo omogućava da broj telefona NN lica sačuvamo i da se uz pomoć jednog „klika“ prikaže ime/ prezime/ fotografija upravo tog lica.

One of the goals of GDPR is that the level of private data protection should be the same within all EU territory.

Until this date – the LPPI has not been aligned with the GDPR.

An interesting occurrence in the days leading up to the local elections in Montenegro held on October 23, 2022, is sending SMS messages to numerous citizens by different political parties.

A number of questions arise in this situation:

1. where have the political parties received the citizen’s numbers from,
2. is the right to citizen’s privacy at stake here,
3. is a phone number a private data, as well as others.

Today’s advanced technology allows us to save an NN’s phone number with the help of apps used daily and with one „click“ have the name / surname / photo of exactly that person.

Građani su primali SMS poruke sa sadržinom i linkom na koji je potrebno kliknuti za pregled sadržaja, odnosno koji vodi do određene stranice. Ovdje možemo govoriti o zajedničkoj odgovornosti operatora i političkih partija koje upravljaju stranicom na društvenim mrežama (fan page) – tzv. „zajednički rukovaoci".

U konkretnom slučaju građani imaju pravo da zahtijevaju i od političkih partija i operatora informacije o podacima koje se prikupljaju putem linkova u SMS porukama, načinu prikupljanja podataka i dozvoljenosti da se podaci o ličnosti uopšte prikupljaju, odnosno dijele sa drugima.

Nezakonito postupanje jednih i drugih bi moglo da rezultira odgovornošću prema građanima za nematerijalnu štetu. Sjetimo se samo slučaja nezakonitog objavljivanja podataka o građanima koja nisu poštovala pravila o izolaciji zbog COVID 19 - u ovom slučaju je sud dosudio građanima pravični iznos naknade.

Citizens received SMS messages with content and link on which it's necessary to click to review content, i.e. which leads to a certain page. Here we can speak of the common responsibility of operators and political parties which manage the page on social networks (fan page) – so-called „joint controllers".

In this case, the citizens have a right to demand from both the political parties and operators, information on which data they collect through links sent in the SMS messages, the manner of collecting data, and authorization to even collect personal data and share it with others.

Illegal actions of one and the other could result in responsibility for immaterial damages to the citizens. Let us remember the case of the illegal publication of private data of citizens which did not respect COVID-19 isolation rules – in this case, the court awarded citizens a righteous remuneration.

U tački 26 Preambule GDPR je navedeno da, kako bi se odredilo da li identitet fizičkog lica može da se odredi, treba uzeti u obzir sva sredstva, kao što je izdvajanje (singling out), koja će rukovalac ili bilo koja druga osoba vjerovatno koristiti za neposredno ili posredno određivanje identiteta fizičkog lica.

Da bi se utvrdilo da li će sredstva određivanje identiteta fizičkog lica vjerovatno da se koriste, treba uzeti u obzir i sve objektivne faktore, kao što su troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir tehnologiju dostupnu prilikom obrade i tehnološki razvoj.

Dakle, da li je broj telefona/ pretplatnički broj dio našeg identiteta i samo naš ili se, ipak, njime mogu služiti i svi oni kojima broj nikada nismo dobrovoljno dali niti potpisali saglasnost za korišćenje u svrhe koje prevazilaze namjenu obrade, a posebno ne u svrhe vođenja političkih kampanja?

Article 26 of GRPR's Preamble states that, to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Therefore, is a phone number / prepaid number a part of our identity and only ours, or, can it be used by all of those to whom we have never voluntarily provided our number with nor signed consent for use in purposes other than processing, and especially not in the purpose of leading political campaigns?

Naravno da operatori mogu da obrađuju naše podatke u svrhu pružanja usluge, odnosno zaključenja i izvršenja pretplatničkog ugovora, a za svaku dalju obradu odnosno dijeljenje podataka moraju da traže naš pristanak.

Ovo je propisano i Zakonom o elektronskom komunikacijama i ZZPL. Isto važi i za političke partije – naši brojevi telefona u bazama operatora mogu samo da koriste ti isti operatori da bi nam pružili uslugu te prikupljanje podataka od strane političkih partija u svrhu vođenja izbornih kampanja bez našeg pristanka je jednostavno - nezakonito.

Građani mogu na jednostavan način da utvrde da li političke partije na osnovu podataka koje imaju o njima mogu da utvrde njihov identitet – tako što će podnijeti zahtjev za obavještenje da rukovalac o njemu obrađuje podatke.

Ukoliko rukovalac ne postupi po zahtjevu, građani mogu podnijeti zahtjev nadzornom organu za ostvarivanje ovog prava odnosno Agenciji za zaštitu ličnih podataka („Agencija“).

Of course, operators can process our data for the purpose of providing service, i.e. conclusion and execution of subscription agreement, and if used for any other purpose i.e. sharing of information, they must receive our consent to it.

This is also determined by the Law on electronic communications and LLPI. The same is for political parties – our phone numbers in operator's data bases can be used by those operators to provide service, and, collecting data by political parties, with the purpose of leading election campaigns, without our consent is simply – illegal.

Citizens can simply determine whether political parties are able to determine their identity, based on the data they have collected about them, – by filling a request and enquiring whether the controller is managing their private data.

If the data controller does not act in accordance with the request, the citizens may submit a request to the supervisory body i.e. Agency for protection of private data („Agency“).

Agencija ima široka ovlašćenja za sprovođenje ZZPL, između ostalih i da pristupi zbirkama podataka o ličnosti i sredstvima elektronske obrade ličnih podataka.

Imajući u vidu sve naprijed rečeno, građani ne bi trebali da olako prelaze preko narušavanja njihove privatnosti.

Naprotiv, ukoliko nisu dali pristanak za obradu podataka o ličnosti, treba da pitaju i operatore i političke partije sa kim se dijele njihovi podaci:

1. zbog čega se dijele ti podaci,
2. koji podaci se dijele/ razmjenjuju,
3. kako i na osnovu čega prikupljaju podatke, odnosno da iskoriste sva zakonom dozvoljena sredstva kako bi zaustavili nezakonitu obradu uz zahtjev za pravičnu naknadu zbog povrede privatnosti.

Agency has a wide scope of authorization to act in accordance with the LLPI, among others, to also access private data collections and means of electronic data processing.

Having in mind all previously stated, citizens should not so easily tolerate breaches of their privacy.

On the contrary, if they have not consented to processing of their private data, they should request information from both operators and political parties with whom their data is shared:

1. why is private data shared,
2. which private data is shared / exchanged,
3. how and based on what are they collecting data, i.e. to use all legally available means to stop illegal processing, alongside a request for righteous remuneration for breach of their privacy.

Ukoliko se privredna društva izdaju da su društveno odgovorna, već je trebalo da svoje poslovanje usklade sa GDPR ne čekajući usklađivanje lokalne regulative, i da na taj način opravdaju povjerenje građana da podatke obrađuju na pošten i zakonit način.

Istraživanja ozbiljnih kuća pokazuju da je povjerenje građana najvažnije za postizanje uspjeha u poslu i u politici i da ulaganje u zaštitu podataka o ličnosti dovodi do povećanja profita kompanija.

Nepoštovanje ZZPL dovodi do skandala i urušavanja ugleda kod javnosti što direktno utiče na gubitak povjerenja i profesionalnu propast.

If commercial entities claim to be socially responsible, they should have aligned their business operations with GDPR, not awaiting alignment of local regulation, thereby justifying the trust, given by the citizens, to process data fairly and in accordance with the law.

Research coming from reputable sources, claims that consumer trust is the most important factor in achieving success in business and politics, and that investing in data protection leads to increased profits.

Breach of LLPI leads to scandals and distortion of reputation with the public, which directly impacts the loss of trust and professional ruin.