Bankarstvo, 2017, vol. 46, br. 4 166
Primljen: 20.10.2017. Prihvaćen: 07.11.2017.

stručni članak

doi: 10.5937/bankarstvo1704166M

Erne Mraznica

Raiffeisen banka ad Beograd
erne.mraznica@raiffeisenbank.rs

GDPR - NOVI IZAZOV ZAŠTITE PODATAKA O LIČNOSTI

Prevod obezbedio autor

Rezime

Dana 4. maja 2016. godine objavljena je Opšta Uredba o zaštiti podataka o ličnosti u Sl. glasniku EU, koja će se primenjivati od 25. maja 2018. godine. Cilj propisa je harmonizacija zaštite podataka o ličnosti na nivou EU, veći stepen kontrole za lica čiji se podaci obrađuju i unapređeno upravljanje savremenim rizicima iz ove oblasti. Banke, po prirodi svog poslovanja, spadaju među najveće rukovaoce podataka o ličnosti i u postupku usklađivanja sa obavezama utvrđenih Uredbom biće u prilici da izvrše punu analizu svog postojećeg regulatornog i infrastrukturnog okvira zaštite podataka o ličnosti. Istovremeno, pruža im se prilika da isprave eventualne nedostatke u postojećim procesima, odnosno da značajno povećaju svest organizacije o standardima zaštite podataka o ličnosti, posebno imajući u vidu zaprećene stroge sankcije za slučaj neusklađenosti.

Ključne reči: GDPR, podatak o ličnosti, osnovni principi, prava lica, rukovalac, obrada podataka, transfer podataka, sankcije, usklađivanje

JEL: F52, G14

Bankarstvo, 2017, Vol. 46, Issue 4
Received: 20.10.2017 Accepted: 07.11.2017

doi: 10.5937/bankarstvo1704166M

expert article

Erne Mraznica

Raiffeisen banka ad Beograd
erne.mraznica@raiffeisenbank.rs

GDPR - A NEW CHALLENGE FOR PERSONAL DATA PROTECTION

Translation provided by the author

Summary

On May, 4th 2016 the General Data Protection Regulation (GDPR) was published in the Official Gazette of the EU, which will be in force from May, 25th 2018. The goal of the Regulation is the harmonization of the personal data protection at the EU level, the larger extent of control for the persons whose data are being processed (data subjects) and the improved management of modern risks in this area. Banks, by the nature of their business, are among the largest processors of personal data and during the process of complying with the GDPR will be in the position to conduct a full assessment of their existing regulatory and infrastructural personal data protection framework. At the same time, this will be an opportunity to correct the potential shortcomings in the existing processes and to significantly raise awareness about the organization of personal data protection standards, especially having in mind the strict sanctions in case of non-compliance.

Keywords: GDPR, personal data, basic principles, data subject rights, controller, data processing, data transfer, sanctions, compliance

JEL: F52, G14

Povelja Evropske Unije (EU) o osnovnim pravima utvrđuje da je zaštita fizičkih lica u odnosu na obradu podataka o ličnosti osnovno pravo, odnosno da svako lice ima pravo na zaštitu svojih podataka o ličnosti.

Pravo na zaštitu podataka o ličnosti nije apsolutno pravo, već se mora posmatrati u vezi s funkcijom koju ima u društvu i mora biti uravnoteženo sa drugim osnovnim pravima, u skladu s načelom proporcionalnosti. Cilj EU zakonodavca je donošenje propisa kojim se posebno ističe poštovanje privatnog i porodičnog života, doma i komunikacija, zaštita podataka o ličnosti, sloboda mišljenja, savesti i veroispovesti, sloboda izražavanja i informisanja, sloboda poslovanja, pravo na delotvoran pravni lek i pošteno suđenje, kao i pravo na kulturnu, versku i jezičku različitost.

Usled brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti podataka o ličnosti. Obim prikupljanja i razmene podataka o ličnosti značajno se povećao. Tehnologija omogućava kako privatnim društvima, tako i organima vlasti da koriste podatke o ličnosti u do sada nezabeleženom obimu za potrebe obavljanja svojih poslova. Fizička lica svoje lične informacije sve više čine javno i globalno dostupnima. Tehnologija je preobrazila i privredu i društveni život i dodatno olakšava slobodan protok podataka o ličnosti.

Imajući u vidu navedeno, vremenom se u praksi pojavila potreba za donošenjem jednog savremenog propisa koji bi uredio zaštitu podataka o ličnosti na teritoriji EU, odnosno upravljanje postojećim rizicima u ovoj oblasti.

Nakon najduže rasprave o nekom dokumentu u EU, 4. maja 2016. godine je objavljena Opšta Uredba o zaštiti podataka o ličnosti u Sl. glasniku EU, sa odredbom da će se propis naći u primeni počev od 25. maja 2018. godine.

Osnovni cilj Uredbe je harmonizacija zaštite podataka o ličnosti na nivou EU i veći stepen kontrole za lica čiji se podaci obrađuju. Za razliku od Direktive o zaštiti podataka, koja prethodi Uredbi i koja je stupila na snagu u decembru 1995. godine, Uredba se primenjuje na teritoriji cele EU, bez obaveze članica da donose posebne, lokalne propise o zaštiti podataka o ličnosti.

Cilj propisa je ujedno i usklađivanje regulatornog okvira sa aktuelnim rizicima, pre svega razumevajući i uzimajući u obzir rizike savremenog, internet doba po podatke o ličnosti. Prethodna Direktiva je praktično doneta u rano doba interneta, u vremenu pre postojanja Google-a i svakako nije izdržala korak sa razvojem tehnologije, brzinom, odnosno količinom obrada podataka o ličnosti.

Okvir

Uredba se primenjuje na obradu podataka o ličnosti, u vezi čije definicije uvodi određene izmene upravo u smislu osavremenjivanja. U tom kontekstu, podatkom o ličnosti se smatraju i online identifikatori i IP adrese lica. Na isti način su detaljno opisani i osetljivi podaci o ličnosti u koje spadaju rasno i etničko poreklo, politička, verska i filozofska uverenja, seksualni život i orijentacija, biometrijski podaci, sindikalno članstvo, zdravlje.

Što se tiče teritorijalnog okvira, Uredba se primenjuje na obradu u kontekstu aktivnosti rukovaočevog i obrađivačevog ustanovljenja u EU, bez obzira da li se obrada vrši u EU ili ne. Takođe, Uredba se odnosi i na rukovaoce i obrađivače bez ustanovljenja u EU, ako nude robu ili usluge fizičkim licima u EU ili prate ponašanje fizičkih lica unutar EU.

Osnovni principi

Sedam osnovnih principa Uredbe predstavljaju temelj na kojem će se zaštita podataka o ličnosti u EU zasnivati i oni u značajnoj meri određuju položaj, prava i obaveze rukovaoca, obrađivača i lica čiji se podaci obrađuju.

U odnosu na prethodnu regulativu (Direktiva o zaštiti podataka), značaj primene principa je naglašeniji, definicije su jasnije, a ujedno su proširene određenim, savremenim principima zaštite podataka o ličnosti. Za razliku od prethodne Direktive gde su se principi pre svega odnosili na kvalitet podataka, Uredba principe vezuje za obradu podataka o ličnosti.

Principi Uredbe, koji su u svojoj osnovi obuhvaćeni i prethodnom regulativom, su: princip zakonitosti, fer obrade i transparentnosti, princip ograničenja svrhe, princip minimalne

The European Union (EU) Charter of Fundamental Rights determines that the protection of natural persons regarding the processing of personal data is the basic right and that every person has the right to the protection of his or her personal data.

The right on personal data protection is not an absolute right; it has to be observed in the relation to its function in the society and it has to be balanced with the other basic rights, by applying the principle of proportionality. The goal of the EU regulator was the adoption of a regulation which will bring attention to the respect of private and family life, home and communications, personal data protection, freedom of opinion, conscience and religion, freedom of expression and information, freedom of conducting business, right to an effective legal remedy and fair trial, as well as the right to the cultural, religious and linguistic diversity.

The new challenges for personal data protection have occurred as a result of the rapid technological development and globalization. The volume of personal data collection and transfer has been significantly increased. The technology allows both private companies and public authorities to use personal data for their businesses to the so far unrecorded degree. Natural persons make their personal data more publicly available. Technology has transformed the economy and social life and additionally enabled the free flow of personal data.

Considering the above stated, over time there has been a need for the creation of the modern regulation which would regulate the personal data protection on the territory of the EU and the management of the existing risks in this area.

After the longest discussion regarding a document in the EU, on May, 4th 2016, the General Data Protection Regulation was published in the Official Gazette of the EU, prescribed to come into force starting from May, 25th 2018.

The basic goal of the GDPR is the harmonization of the personal data protection at the EU level and the larger extent of control for the persons whose data are being processed. Unlike the Data Protection Directive, which was the regulation prior to the GDPR, in force since December 1995, the GDPR is applicable throughout the EU territory, without the obligation of the member states to adopt any special, local personal data protection regulations.

At the same time, the goal of the Regulation is the compliance of the regulatory framework with the existing risks, especially concerning the identification and consideration of the risks of the modern, internet era in relation to the personal data. The prior regulation was adopted in the early internet era, in the pre-Google time and understandably, it did not keep up with the technological development, the speed and volume of the personal data processing.

Framework

The GDPR refers to the processing of personal data by introducing certain changes to its definition, with the purpose of its modernization. In that context, online identifiers and personal IP addresses are recognized as personal data as well. In the same way, the sensitive personal data, including racial and ethnic origin, political, religious and philosophical beliefs, sexual life and orientation, biometric data, syndicate membership, health, are being described into more detail.

Regarding the territorial framework, the GDPR is being applied to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. Additionally, the GDPR applies even to the controllers and

obrade podataka, princip tačnosti, princip ograničenja pohranjivanja podataka. Međutim, **princip integriteta i poverljivosti** predstavlja tekovinu Uredbe i obuhvata zaštitu podataka tehničkim i organizacionim merama, obaveštavanje nadzornog organa i lica čiji su podaci u slučaju prodora u bezbednost podataka. Ipak, verovatno najvažniji princip jeste **princip odgovornosti,** koji uvodi obavezu rukovaoca da dokaže da se pridržava svih principa. Samo obveznici koji sa uspehom mogu dokazati da su usklađeni će izbeći odgovornost za eventualne nepravilnosti u primeni propisa.

Prava lica čiji se podaci obrađuju

Lice čiji se podaci o ličnosti obrađuju je centralna figura Uredbe. Spektar prava koji se pruža licu omogućiće mu, pod uslovom odgovarajuće primene propisa, pre svega kontrolu u značajnoj meri o tome kom će rukovaocu/obrađivaču dati podatke, koliko podataka i za koji period. Spektar prava lica čiji se podaci obrađuju bi se mogao svesti na pravo na: obaveštenje o obradi, pristup podacima, ispravku**,** prigovor, brisanje podataka (pravo da podaci budu zaboravljeni), obustavu obrade**,** prenosivost podataka, u vezi automatskog odlučivanja, reklamaciju**,** sudsku zaštitu, obeštećenje. Određena prava se po svojoj prirodi i načinu regulisanja nameću kao ona od suštinskog značaja, kako iz perspektive lica čiji se podaci obrađuju, tako i iz ugla rukovaoca i obrađivača koji će biti u obavezi da po tim pravima postupaju. U tom kontekstu izdvajaju se:

- **Pravo na obaveštenje o obradi** - sadrži obavezu rukovaoca i obrađivača da sastave detaljno obaveštenje o obradi prilikom prikupljanja podataka, koji će sadržati osnov i svrhu obrade, informaciju o eventualnom transferu podataka, o vremenu čuvanja, pravima lica. Naglašeno je da obaveštenja moraju biti napisana jasnim, jednostavnim jezikom, sa podacima o rukovaocu/obrađivaču i licu za zaštitu podataka o ličnosti.
- **Pravo na brisanje podataka** - pod uslovom da podaci nisu neophodni za svrhu obrade, da je povučen pristanak lica, da nema osnova za obradu.
- **Pravo na prenosivost podataka** - jedna od novina Uredbe, prenos od jednog do drugog rukovaoca, pod uslovom da su podaci u formatu koji omogućava mašinsko očitavanje, da postoje tehničke mogućnosti, da se radi o automatizovanoj obradi podataka.

Jasno je da će puna primena opisanih prava lica čiji se podaci obrađuju predstavljati izazov za rukovace i obrađivače. Potrebno je naglasiti da se sva navedena prava mogu ograničiti radi poštovanja i zaštite javnog interesa, odnosno interesa kao što su državna bezbednost, odbrana, javna sigurnost, sudski postupak.

processors without an establishment in the EU, if they offer goods or services to natural persons in the EU or monitor the behavior of natural persons within the EU.

Basic Principles

Seven basic principles of the GDPR represent the foundation on which the personal data protection in the EU will be based and they significantly determine the status, rights and duties of controllers, processors and persons whose data are being processed.

In comparison with the prior regulation (Data Protection Directive), the GDPR stresses the importance of the implementation of principles to a higher degree; the definitions are more transparent and broadened by means of the certain, modern principles of personal data protection. Unlike the prior regulation, where the principles were related to the data quality, the GDPR connects the principles to the personal data processing.

The GDPR principles which were essentially included in the prior regulation as well are: lawfulness, fairness and transparency of processing, purpose limitation, data minimization, accuracy, and storage limitation. However, the **principle of integrity and confidentiality** is the heritage of the GDPR and it includes the technical and organizational measures for data protection, notifications to the regulatory authority and data subjects in case of security breaches. Still, the **principle of accountability** is probably the most important principle, which introduces the duty of a controller to confirm compliance with all the principles. Only the obligors who can successfully prove compliance will avoid the responsibility for the potential omissions in the implementation of the regulation.

Data Subjects' Rights

A data subject is the central figure of the GDPR. The spectrum of rights provided to a person will enable him/her, under the condition that the regulation is properly implemented, a significant level of control when it comes to the choice of the controller/processor to which he/she will provide data, the extent of the provided data and the relevant period. The spectrum of rights of data subjects can be reduced to the following rights: the right to be informed about the processing, the right to data access, rectification, objection, erasure (right to be forgotten), restriction of processing, data portability, automated decision making, complaint, judicial protection, remedy. Certain rights, by their nature and model of regulation, are imposed as the ones with crucial relevance, from the perspective of a person whose data are being processed and controllers/processors who are obliged to act upon the described rights. In that context the following rights stand out:

- **The right to be informed about the processing** - refers to the controllers' and processors' obligation to prepare a detailed notification about the processing during the collection of data, which will contain the basis and the purpose of the processing, the information on the potential transfer of data, the period of data storage, the persons' rights. The Regulation stresses that the notifications have to be written in a clear, simple manner, and contain the information about the controller/processor and the data protection officer.
- **The right to data erasure** - under the condition that the data are not necessary for the purpose of the processing; the consent of a person is being withdrawn; there is no basis for processing.
- **The right to data portability** - one of the novelties of the GDPR; transfer of data from one to another controller, if the data are in the format which allows machine readability, if there are the required technical possibilities and the processing is carried out by automated means.

It is clear that the full application of the described rights of data subjects will be challenging for the controllers and processors. It is important to highlight that all of the mentioned rights can be limited due to the respect and protection of public interests, i.e. interests such as national security, public safety and judicial procedures.

Controller/Processor

The GDPR introduces the new obligations

Rukovalac/obrađivač

Uredba je uvela nove pojmove i standarde koji uređuju položaj i obaveze rukovaoca/obrađivača, a koji se pre svega odnose na implementaciju odgovarajućih tehničkih i organizacionih mera kako bi se sa jedne strane obezbedila obrada podataka o ličnosti u skladu sa propisom, a da se istovremeno na osnovu tih mera bez teškoća demonstrira usklađenost sa Uredbom, za slučaj regulatornog nadzora.

Značajni novi pojmovi i standardi Uredbe su:

- **Ugrađena zaštita podataka** (*privacy by design*) - rukovalac u vreme razvijanja softvera ili njegove primene uvodi odgovarajuće mere zaštite podataka, koje čine podatke neprepoznatljvim za neovlašćena lica. Moguće mere zaštite podataka u navedenom kontekstu su pseudonimizacija ili enkripcija podataka, koje su osmišljene za delotvorno sprovođenje načela zaštite podataka.
- **Podrazumevana zaštita podataka** *(privacy by default)* - privatnost preventivno ugrađena u sistem/aplikaciju, primenjena restriktivna svha obrade i ne postoji potreba za dodatnom zaštitom tehničkim sredstvima. Rukovalac primenjuje odgovarajuće tehničke i organizacione mere kojima se obezbeđuje da se podrazumevana obrada vrši samo nad podacima o ličnosti koji su neophodni za konkretnu svrhu obrade. Ova obaveza se odnosi na količinu prikupljenih podataka o ličnosti, obim njihove obrade, rok njihovog čuvanja i njihovu dostupnost.

  Konkretno, tim merama se obezbeđuje da podaci o ličnosti ne budu automatski, bez intervencije lica, dostupni neograničenom broju fizičkih lica.
- **Procena uticaja obrade na zaštitu podataka** - je obavezna kada obrada predstavlja visok rizik za prava lica, posebno kada se radi o primeni novih tehnologija prilikom obrade, profilisanja, opsežnih obrada. Listu obrada obaveznih za procenu sastavlja regulatorni organ.
- **Lice za zaštitu podataka o ličnosti** - čije je imenovanje obavezno u slučaju da obrada sadrži redovno, sistematično i opsežno praćenje lica ili se delatnost obveznika sastoji od opsežne obrade osetljivih podataka. Uslovi za imenovanje su profesionalni kvaliteti lica, a posebno ekspertsko znanje iz oblasti zaštite podataka o ličnosti. Može biti i lice angažovano eksterno. Predstavlja kontakt osobu za lica čiji se podaci obrađuju i regulatora.
- **Prodor u bezbednost podataka** - ukoliko utvrdi da postoji rizik za prava lica, rukovalac je u obavezi da obavesti državni organ u roku od najkasnije 72 sata od saznanja za prodor. U slučaju da rukovalac utvrdi visok rizik za prava i slobode fizičkih lica obaveštava lice čiji se podaci obrađuju bez odlaganja.

Pored navedenih instituta značajnu novinu predstavlja mogućnost pribavljanja sertifikata o kvalitetu standarda zaštite podataka o ličnosti, koju izdaje sertifikaciono telo ovlašćeno od strane nadležnog regulatora na period od tri godine.

Transfer podataka

Cilj odredaba o transferu podataka iz EU je obezbeđivanje zaštite zajemčene Uredbom i kada se podaci obrađuju van EU. Podaci se prenose fizički, putem iznošenja nosača podataka ili elektronski, putem omogućavanja pristupa podacima. Postoje različiti kriterijumi na osnovu kojih je omogućen transfer, bez posebne odluke o odobravanju transfera od strane regulatornog organa. To su, pre svega, odluke o adekvatnosti kojima Evropska komisija potvrđuje da treća strana kojoj se šalju podaci obezbeđuje adekvatni nivo zaštite; zatim, akti koji garantuju primenu, kao što su međunarodni sporazumi, klauzule EU, sertifikati, obavezujuća korporativna pravila, kodeksi ponašanja. Pored navedenog, postoje i izuzeci u posebnim situacijama, te je tako omogućen transfer podataka o ličnosti uz izričit pristanak lica, radi izvršenja ugovornih obaveza, javnog interesa, ubedljivog legitimnog interesa rukovaoca, uz obavezno obaveštavanje regulatornog organa o transferu i zaštitnim merama.

Navedeno jasno nameće zaključak da je za velike multinacionalne organizacije svrsishodno da zaključe odgovarajuće akte kojima garantuju primenu visokih standarda zaštite podataka o ličnosti u okviru svojih grupacija i time omoguće sebi transfer podataka između svojih članica.

and terms which regulate the status and duties of controllers/processors and which primarily refer to the implementation of appropriate technical and organizational measures, so that the processing of personal data in line with the regulation is ensured, but that based on these measures, an organization can at the same time easily demonstrate compliance with the GDPR, in case of regulatory supervision.

Important new terms and obligations of the GDPR are:

- **Privacy by design** - controller, at the time of the software development or its implementation, introduces the appropriate measures of data protection, which make the data unrecognizable for unauthorized persons. The possible protection measures in the mentioned context are pseudonymisation or encryption of data, which are created for the effective implementation of the data protection principles.
- **Privacy by default** - privacy is preventively built into the system/application; the restrictive purpose of processing is implemented and there is no need for additional protection by technical means. The processor applies the proper technical and organizational measures which, by default, ensure that processing is conducted only in respect of the personal data necessary for the purpose of processing. This obligation refers to the quantity of the collected personal data, extent of processing, period of storage and their availability.

  In particular, these measures ensure that personal data do not become available to an undetermined number of persons automatically, without a person's intervention.
- **Data protection impact assessment** - the assessment is mandatory when processing represents a high risk for the persons' rights, especially where new technology is being used for the purpose of processing, profiling, and large scale processing. The regulator creates a list of processing cases for which the impact assessment is mandatory.
- **Data protection officer** - must be appointed in case when the processing involves the regular, systematic and extensive monitoring of persons or when the core activity of the obligor contains extensive processing of sensitive data. The conditions for the appointment are the professional qualities of a person, especially their expert knowledge in the area of personal data protection. The person can be engaged externally. He/she represents the contact person for the data subjects and for the regulator.
- **Breaches into data security** - if the processor assesses that there is a risk for the rights of persons, he is obliged to notify the supervisory authority within 72 hours since he has been informed about the breach. In case the processor assesses a high risk for the rights and freedom of natural persons, he notifies without delay the persons whose data are being processed.

In addition to the mentioned terms and obligations, an important novelty is the possibility to acquire a certificate on the quality of the personal data protection standards, which is issued by the certification body authorized by the competent regulator for the period of three years.

Data Transfer

The goal of the provisions on data transfer from the EU is to ensure the protection provided by the GDPR when the data are being processed outside of the EU. The data are transferred physically, by data carrier or electronically, by providing data access. There are different criteria based on which the transfer is enabled, without a special decision about the approval of transfer by the regulator. Those are primarily adequacy decisions by which the European Commission confirms that the third party to whom the data are being sent ensures the adequate level of protection, along with the acts which guaranty the application, such as international treaties, EU clauses, certificates, binding corporate rules, codes of conducts. Besides the above mentioned, there are some exceptions in special situations such as transfers based upon an explicit consent of a person, for the purpose of enforcing the contractual obligations, sustaining a public interest, or a legitimate interest of the processor, with a mandatory notification sent to the supervisory authority about the concerned transfer and

Sankcije

Jedna od glavnih karakteristika Uredbe, i čini se, način na koji je skrenuta pažnja javnosti na propis, je pooštren režim administrativnih, novčanih kazni, za slučaj neusklađenosti sa obavezama. U zavisnosti od vrste prekršaja kazne se izriču u visini do 10 miliona EUR, ili u slučaju kompanija do 2% ukupnog godišnjeg prometa na svetskom nivou za prethodnu finansijsku godinu. Ove kazne se mogu izreći za nepravilnosti u vezi tehničke, organizacione osposobljenosti, vođenja evidencija, procene uticaja, imenovanja lica i dr.

Do visine od 20 miliona EUR, ili u slučaju kompanija do 4% ukupnog godišnjeg prometa na svetskom nivou za prethodnu finansijsku godinu, kazne se od strane regulatornog organa mogu izreći za povrede osnovnih principa obrade, prava lica, transfera podataka, nepostupanja po naredbi nadzornog regulatora. Pored navedenih novčanih kazni, nadzornom regulatornom telu na raspolaganju su i odgovarajuće mere koje se kreću od korektivnih mera usklađivanja rukovaoca sa propisanim obavezama, do mogućnosti zabrane dalje obrade, transfera, naloga za brisanjem podataka, ispravkom, pa i do oduzimanja sertifikata kvaliteta.

Usklađivanje

Republika Srbija je u statusu kandidata za EU i započeti su pregovori o pristupanju EU u kom postupku je Republika Srbija u obavezi da usvoji pravne tekovine EU. Poglavlje 23 pristupnih pregovora se odnosi na oblast Pravosuđa i osnovnih prava. U okviru ovog Poglavlja od Republike Srbije se zahteva usklađivanje propisa iz oblasti zaštite podataka o ličnosti. Tokom marta meseca tekuće godine, Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti objavio je novi model Zakona o zaštiti podataka o ličnosti koji je u značajnoj meri usklađen sa principima Uredbe. Javna rasprava o predloženom modelu zakona okončana je tokom aprila meseca tekuće godine i u narednom periodu se očekuje da isti preko nadležnog Ministarstva pravde uđe u redovni postupak usvajanja.

Zaključak

Ono što banke kao potencijalni budući obveznici Uredbe mogu preduzeti u periodu pred početak primene propisa, a radi efikasnog usklađivanja sa opisanim obavezama je, u kratkim crtama, sledeće:

1. Imenovanje lica za zaštitu podataka o ličnosti;
2. Utvrđivanje činjeničnog stanja, primenom pristupa baziranog na proceni rizika (utvrdjivanje koji postupci obrade podataka o ličnosti postoje u njihovoj organizaciji, koji je njihov rizik, uz adekvatno dokumentovanje rezultata);
3. Provera usklađenosti svih identifikovanih radnji obrade podataka o ličnosti sa propisima;
4. Izmena dokumenata, postupaka, sistema (obaveštenja o obradi, obrasca saglasnosti lica za obradu podataka, ugovornih odredbi sa dobavljačima, IT arhitektura, baze podataka);
5. Provera sistema bezbednosti podataka (enkripcija, pseudonimizacija, tehnička i organizaciona osposobljenost, uređivanje postupka za slučaj prodora u bezbednost podataka);
6. Izrada smernica za primenu principa ugrađene, odnosno podrazumevane zaštite podataka.

Imajući u vidu prethodna iskustva prilikom primene važećeg Zakona o zaštiti podataka o ličnosti, odnosno primene obaveze čuvanja bankarske tajne i razvijene sisteme bezbednosti podataka, kada se radi o primeni načela i obaveza istaknutih u Uredbi, banke u Srbiji su svakako

respective safeguards.

The above described practice leads to the conclusion that for large multinational companies it is adequate to conclude relevant acts which would serve as a guarantee of the application of high personal data protection standards within their group, thereby enabling the transfer of data among their members.

Sanctions

One of the main characteristics of the GDPR and, obviously, the way how the public attention was drawn to the regulation, is the strict regime of administrative fines, in case of non-compliance with the obligations. Depending on the type of infringement, the fines can go as high as 10 million EUR, or in case of corporates up to 2% of their total annual worldwide turnover from the preceding financial year. These fines can be imposed for infringements regarding the technical and organizational capabilities, record keeping, impact assessment, data protection officer appointment, etc.

For the infringement of the basic principles of processing: rights of persons, data transfer, failure to comply with the orders of supervisory authorities, the supervisory authority can impose fines up to 20 million EUR or in case of corporates up to 4% of their total annual worldwide turnover from the preceding financial year. Besides the mentioned fines, the supervisory authority can also impose proper measures for the processor, ranging from the corrective measures of compliance with the obligations to the potential suspension of further data processing, transfer, erasure, rectification, or even withdrawal of the quality certificate.

Compliance

The Republic of Serbia has the status of a candidate for joining the EU and the negotiations on joining the EU have started. In this process the Republic of Serbia is obliged to adopt the legal heritage of the EU. Chapter 23 of the negotiations refers to the area of judiciary and fundamental rights. In the scope of this Chapter, the Republic of Serbia is also required to harmonize the regulations in the area of personal data protection. During March this year the Commissioner for Information of Public Importance and Personal Data Protection published a new draft of the Law on Personal Data Protection, which is to a large extent compliant with the principles of the GDPR. The public discussion concerning the draft law has been completed during April this year and in the following period the Ministry of Justice is expected to initiate the regular process of its adoption.

Conclusion

In order to effectively comply with the described regulation, what banks as potential future obligors of the GDPR can undertake is, in short, the following:

1. Appointment of a Data Protection Officer;
2. Identification of the factual status, by applying the risk based approach (identification of processes of personal data processing existing in their organization and their risks, accompanied by the proper documentation of results);
3. Compliance analysis of all identified processes of personal data processing with the regulations;
4. Amending of documents, processes, systems (notifications of processing, template for a person's consent to data processing, contractual clauses with suppliers, IT architecture, databases);
5. Data security system check (encryption, pseudonymisation, technical and organizational capacity, definition of the process in case of data security breaches);
6. Creation of guidelines for the implementation of the Privacy by Design and Privacy by Default principles.

Considering prior experiences in the implementation of the existing Law on Personal Data Protection and the application of banking secrecy and developed data security systems, when it comes to the implementation of principles and obligations pointed out in the GDPR, the banks in Serbia have a great advantage in comparison to other obligors from other business fields.

The issue which banks must resolve prior to the GDPR application is whether the regulation applies to the obligors outside the

u prednosti u odnosu na obveznike iz drugih oblasti poslovanja.

Pitanje na koje banke moraju pronaći odgovor pre početka primene Uredbe jeste da li se odredbe Uredbe odnose na obveznike koji se nalaze van teritorije EU. Odgovor na ovo pitanje se nalazi u tumačenju odredbe člana 3. Uredbe kojim je, između ostalog, utvrđeno da se Uredba odnosi i na rukovaoce i obrađivače bez ustanovljenja u EU, ako nude robu ili usluge licima u EU ili prate ponašanje lica unutar EU. Ovo znači da je neophodno izvršiti analizu svih proizvoda banke, odnosno baze klijenata kako bi se utvrdilo koliki je broj klijenata banke u EU, odnosno koje proizvode banka nudi klijentima sa teritorije EU. Ukoliko se analizom utvrdi da banka nudi proizvode klijentima iz EU, koji se mogu koristiti na teritoriji EU, postoje razlozi da nadležni regulatorni organi iz EU utvrde obavezu primene Uredbe u konkretnom slučaju.

Na kraju, umesto zaključka, iz perspektive autora ovog teksta odgovarajući bi bio jedan savet svim budućim Licima za zaštitu podataka o ličnosti, odnosno licima koja će biti zadužena za usklađivanje i nadzor nad primenom Uredbe, a to je da dobro iskoriste ovu priliku i postojeću pažnju najvišeg rukovodstva za podizanje svesti o pitanjima zaštite podataka o ličnosti radi dobijanja adekvatne podrške i resursa neophodnih za primenu ovog novog EU propisa.

Literatura / References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
2. Charter of fundamental rights of the European Union (2007/C 303/01)
3. Directive 95/46/ec of the European Parliament and of the Council 95/46/EZ of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

EU territory. The answer to this question is in the interpretation of Article 3 of the GDPR which, inter alia, determines that the GDPR applies to processors and controllers without an establishment in the EU, if they offer goods and services to the persons in the EU or monitor the behavior of persons within the EU. This means that a detailed analysis of all banks' products and client databases must be performed in order to precisely determine how many EU based clients the bank has, i.e. which products the bank is offering to the clients from the EU territory. If the analysis confirms that the bank is offering products to the clients from the EU, which are being used on the EU territory, there are grounds for the competent supervisory authority of the EU to determine the obligation of the GDPR application in the specific case.

At the end, instead of a conclusion, from the perspective of the author of this text, an advice to all future Data Protection officers and persons who will be responsible for the harmonization and supervision of the GDPR implementation is to use this opportunity and the existing attention of the top management to raise awareness about the personal data protection issues and get the adequate support and resources necessary for the implementation of this new EU regulation.