# #TARABICA
## IT CONFERENCE

Belgrade May 25th, 2019

# GDPR I INFORMACIONE TEHNOLOGIJE

Bogdan Ivanišević, BDK Advokati

Milica Basta, BDK Advokati

Belgrade

May 25th, 2019

# Primena GDPR na rukovaoce i obrađivače u Srbiji

# PRIMENA GDPR-a NA AKTIVNOSTI PROGRAMERA I ADMINISTRATORA U SRBIJI

*Article 3*

*Territorial scope*

*1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

*2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

*(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

*(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

*3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

# PRIMENA GDPR-a NA AKTIVNOSTI PROGRAMERA I ADMINISTRATORA U SRBIJI

GDPR se primenjuje kada programeri ili administratori:

- obrađuju podatke o ličnosti radeći za IT ili drugu kompaniju (npr. osiguravajuću kompaniju) iz EU – bilo da to čine kao freelanceri, u okviru ogranka te EU kompanije u Srbiji, ili u okviru posebne kompanije u Srbiji koju je EU kompanija osnovala; ili

- rade za srpsku kompaniju koja u svojstvu *cloud provider*-a (obrađivač) pruža cloud computing usluge kompaniji (rukovaocu) iz EU.

- rade za kompaniju – bilo odakle da je (npr. iz Srbije, ili iz SAD) – koja nudi robu ili usluge licima u EU, ili prati njihovo ponašanje u EU, i pri tome je obrada podataka o ličnosti, koju sprovodi, u vezi sa tim nuđenjem usluga, odnosno praćenjem ponašanja.

# Principi obrade

# PRINCIPI OBRADE PODATAKA O LIČNOSTI OD NAROČITOG ZNAČAJA ZA IT SEKTOR

- zakonitost … i transparentnost – podaci o ličnosti moraju se obrađivati zakonito … i transparentno u odnosu na lice na koje se podaci odnose;
- ograničenje u odnosu na svrhu obrade – podaci se mogu prikupljati samo u svrhe koje su konkretno određene (*specified*) i izričite (*explicit*) … i ne mogu se dalje obrađivati na način koji nije u skladu sa tim svrhama;
- minimizacija podataka – podaci o ličnosti moraju biti relevantni i ograničeni na ono što je neophodno u odnosu na svrhu obrade;
- ograničenje čuvanja – podaci se smeju čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade; i
- integritet i poverljivost – podaci o ličnosti moraju se obrađivati na način koji obezbeđuje njihovu odgovarajuću zaštitu, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja, primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera.

# PRINCIPI PRETOČENI U OPERATIVNE ODREDBE

Princip zakonitosti … i transparentnosti, pretočen u odredbe o:

- osnovama za zakonitu obradu (pristanak, ispunjenje ugovora, legitiman interes); i
- (rukovaočevom) pružanju detaljnih informacija o obradi i o ostvarivanju prava lica, na sažet, transparentan, razumljiv i lako dostupan način, i sa uključivanjem obaveznih elemenata u sadržaj informacija.

Princip integriteta i poverljivosti, pretočen u odredbe o zaštiti podataka od gubitka, dolaženja u ruke neovlašćenih lica, izmene, i uništenja.

# PRINCIPI KOJI SU PRETOČENI U OPERATIVNE ODREDBE

Princip minimizacije podataka, pretočen u odredbe o:

- data protection by design (projektovana zaštita) – rukovalac je prilikom određivanja načina obrade, kao i u toku obrade, dužan da primeni odgovarajuće tehničke i organizacione mere, kao što je pseudonimizacija, koje imaju za cilj obezbeđivanje delotvorne primene načela zaštite podataka o ličnosti, kao što je smanjenje količine podataka; i
- data protection by default (ugrađena zaštita) – rukovalac je dužan da stalnom primenom odgovarajućih tehničkih i organizacionih mera obezbedi da se od početka obrađuju samo oni podaci o ličnosti koji su neophodni za ostvarivanje svake određene (specific) svrhe obrade. Ta se obaveza primenjuje u odnosu na broj prikupljenih podataka, obim njihove obrade, rok njihovog pohranjivanja i njihovu dostupnost. Tehničkim i organizacionim merama mora se obezbediti da se bez učešća lica podaci o ličnosti ne mogu učiniti dostupnim neograničenom broju drugih lica.

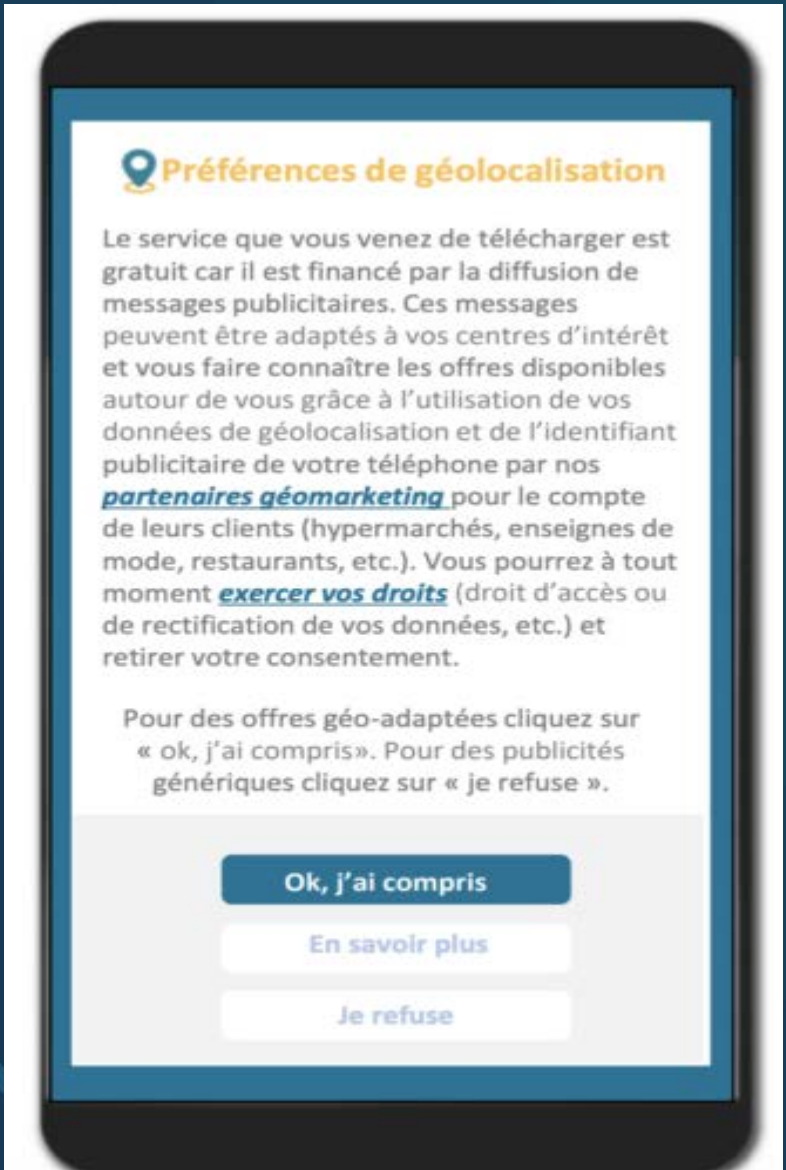
# GDPR PRINCIPI KAO IZAZOV ZA IT SEKTOR

**Pristanak (kao osnov za zakonitost obrade)**

Informisani pristanak:

- *Big Data* - lice nekada ne može dobiti informisan pristanak jer sam rukovalac nije u mogućnosti da licu ponudi dovoljno određenu informaciju o obradi (usled nemogućnosti da precizno odredi svrhu);
- kompanije koje koriste *cookies* i *software development kit* (SDK omogućava prikupljanja podataka o korisnikovoj lokaciji) ne obaveštavaju korisnika – uopšte, ili na razumljiv način – o identitetu trećih lica koja imaju pristup prikupljenim podacima (*TEEMO* odluka francuskog CNIL-a, jun 2018); i
- IoT - lice često ni ne zna da pružalac IoT usluge stavlja podatke na raspolaganje trećim licima.

# GDPR PRINCIPI KAO IZAZOV ZA IT SEKTOR



# GDPR PRINCIPI KAO IZAZOV ZA IT SEKTOR

**Pristanak (kao osnov za zakonitost obrade)**

Slobodno dat pristanak:

- IoT – prema GDPR-u, pružalac usluge ne sme da uslovljava pružanje usluge korisnikovim davanjem pristanka na obradu podataka o ličnosti.

Uopšte dat pristanak:

- korisnik stvari nekada ne zna da je to "povezana stvar", tj. da prikuplja podatke o licu.

# GDPR PRINCIPI KAO IZAZOV ZA IT SEKTOR

**Određenost svrhe** – rukovalac koji obrađuje *Big Data* (generisane kroz, npr., postovnje na socijalnim mrežama, internet pretrage, kupovinu kreditnom karticom, ili upotrebu povezanog automobila ili mobilnog telefona koji geolocira lice) često nema unapred određenu/konkretnu svrhu koju želi ostvariti obradom podataka.

**Minimizacija podataka** – IoT i *Big Data* analitika deluju na suprotnom principu (obrade velike količine podataka).

**Ograničenje perioda čuvanja** – u nekim oblicima *Big Data* analitike cilj je čuvati podatke kroz duži period.

# PRIMENA MERA BEZBEDNOSTI PRILIKOM OBRADE PODATAKA O LIČNOSTI

GDPR izričito pominje samo neke od konkretnih bezbednosnih mera (enkripcija i pseudonimizacija).

Niz drugih mera su stvar prakse i ocene nadzornog tela u konkretnom slučaju (ograničavanje broja administratora ovlašćenih da pristupaju podacima o ličnosti; zabrana deljenja istog administratorskog passworda (administrator password); beleženje aktivnosti u vezi sa podacima; multi-faktorna autentifikacija, jak korisnički password, informisanje korisnika o neuspelim pokušajima logovanja).

Treba koristiti mere koje su skladu sa nivoom tehnoloških dostignuća u datoj oblasti (npr. ažurirane softvere), pri čemu je dovoljno da troškovi primene bezbednosnih mera budu u skladu sa finansijskom snagom rukovaoca, odnosno obrađivača.

# PRIMENA MERA BEZBEDNOSTI PRILIKOM OBRADE PODATAKA O LIČNOSTI

**Posledice nepreduzimanja odgovarajućih bezbednosnih mera**

- *data breach* (koji može kod lica izazvati stres usled neizvesnosti u pogledu mogućih posledica, a može i rezultirati imovinskim posledicama); i
- administrativne kazne (*Rousseau* odluka italijanskog *Garante*-a, april 2019).

# *Data protection impact assessment*

# *DATA PROTECTION IMPACT ASSESSMENT* (DPIA)

Rukovalac (korisnik *cloud computing* usluge, istraživač *Big Data*, pružalac IoT usluge, korisnik *cookies*) je obavezan da pre otpočinjanja obrade uzme sve gore navedeno u obzir u okviru razmatranja da li je potrebno da sprovede procenu uticaja na zaštitu podataka o ličnosti (*data protection impact assessment* (DPIA)), i tokom sprovođenja DPIA.

DPIA zahteva angažovanje znatnog vremena i sredstava na strani rukovaoca. Takođe, obrađivač ima obavezu da pomogne rukovaocu u izvršavanju obaveza u vezi sa DPIA.

# *DATA PROTECTION IMPACT ASSESSMENT* (DPIA)

Minimalni sadržaj DPIA (iz teksta GDPR-a, čl. 36 (7)):

- *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *an assessment of the risks to the rights and freedoms of data subjects […]; and*
- *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

# *DATA PROTECTION IMPACT ASSESSMENT* (DPIA)

Smernice Evropskog odbora za zaštitu podataka o ličnosti, o tome da li korišćenje novih tehnologija, obrada podataka o lokaciji lica, i obradi korišćenjem uređaja sa senzorima, obavezuje na sprovođenje DPIA

Nacionalna nadzorna tela su izradila liste sa radnjama obrade kod kojih se DPIA mora koristiti. Evropski odbor za zaštitu podataka o ličnosti je korigovao liste, pojasnivši sledeće:

- među osnovima koji, svaki sam za sebe, stvara obavezu obaveznog sprovođenja DPIA, su:
  - praćenje ponašanja fizičkog lica i njegove lokacije;
  - match-ovanje podataka ili kombinovanje skupova podataka iz različitih izvora; i
  - profilisanje fizičkih lica u velikom obimu;

# *DATA PROTECTION IMPACT ASSESSMENT* (DPIA)

- korišćenje novih ili inovativih tehnologija nije sami po sebi osnov za obavezno sprovođenje DPIA, ali u sadejstvu sa bar još jednim kriterijumom iziskuje tu obavezu; i

- obrada korišćenjem uređaja sa senzorima, koji prenosi podatke putem interneta ili neke druge tehnologije za prenos podataka, nije kriterijum za obavezno sprovođenje DPIA, ni sama ni zajedno sa drugim kriterijumima. (Umesto toga, u konkretnom slučaju treba ispitati da li izaziva visok rizik).

# Ugovori o obradi podataka

# UGOVORI O OBRADI PODATAKA (*DATA PROCESSING AGREEMENTS*)

Programeri i administratori iz država van EU su obično obrađivači, ili angažovani kod obrađivača, podataka o ličnosti.

Propisana je obaveza da rukovalac iz EU i obrađivač van EU zaključe ugovor koji detaljno reguliše obaveze obrađivača.

Obrada bez ugovora povlači rizik kažnjavanja.

# Cloud serveri van EU: da li je iznošenje dopušteno?

# *CLOUD IZVAN E.U.*

Ako podaci prilikom pružanja *cloud computing* usluge odlaze i u države izvan EU, pod kojim uslovima je takvo iznošenje dopušteno?

Konsekventan pristup bi bio: ako cloud provider nije "pokriven" SCCs-om, niti država *adequacy*-ijem, korišćenje tog cloud-a je nedopušteno.

Predlozi: ograničavanja obrade samo u državama EEA ili EU; standardne ugovorne klauzule; obavezujuća poslovna pravila

# Hvala!

| BDK Serbia | BDK Montenegro | BDK Bosnia and Herzegovina |
|---|---|---|
| Bulevar kralja Aleksandra 28<br>11000 Belgrade<br>T: +381 11 3284 212<br><br>office@bdkadvokati.com | Cetinjska 11<br>The Capital Plaza<br>81000 Podgorica<br>T/F: +382 20 230 396<br><br>office.cg@bdkadvokati.com | Gundulićeva 6<br>78000 Banja Luka<br>T: +387 51 250 641 F: +387 51 250 642<br>office.banjaluka@bdkadvokati.com |

# Sponzori

Generalni sponzor

Microsoft

Partner konferencije

Univerzitet Singidunum

Srebrni sponzori

zühlke empowering ideas

Merit SOLUTIONS

asseco

VEGA IT SOURCING

Bronzani sponzor

ENGINEERING

Tehnički sponzori

Merit SOLUTIONS

SBB SOLUTIONS

trs

Vidimo se / See you soon

#tarabica'19