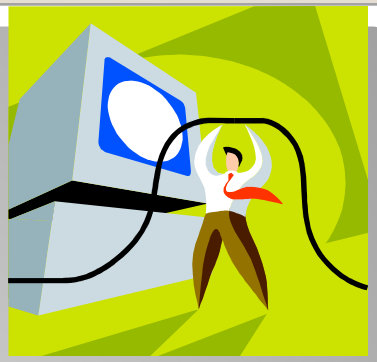
Digitalni svet i PUKOS
Beograd
25. i 26 april 2018.g.

General Data Protection Regulation-GDPR i primena u Srbiji

Dr Dragan Prlja

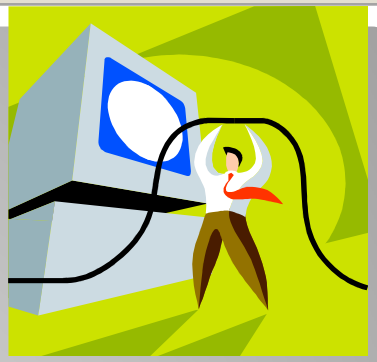
Šta su podaci o ličnosti ?



- Svi podaci kojim se identifikuju fizička lica ili se mogu identifikovati (ime i prezime, identifikacioni broj, lokacijski podaci, zdravstveni,ekonomski, socijalni, itd.)

- IKT podaci: online identifikacija, identifikacija uređaja, identifikacija putem kolačića, IP adrese, elektronska pošta, istorija pretraživanja, logovanja, osetljivi, uključuju genetske i biometrijske podatke (otisak prsta, prepoznavanje lica)

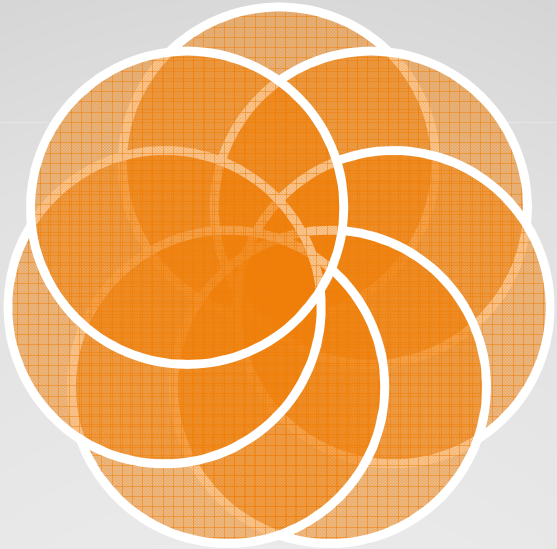
Propisi EU o zaštiti podataka



1981 Konvencija Saveta Evrope o zaštiti pojedinaca od automatizovane obrade podataka o ličnosti

1995 Direktiva o zaštiti građana u vezi sa obradom podataka o ličnosti i o slobodnom kretanju takvih podataka

2016 Opšta uredba o zaštiti podataka (GDPR)



1997 Direktiva Evropske unije o telekomunikacijama

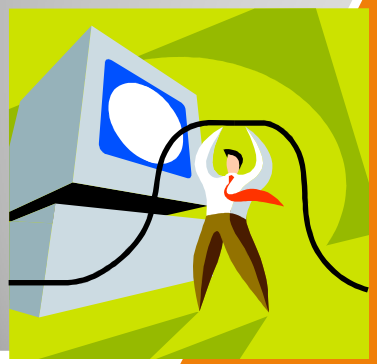
2009 Telekom Paket Direktiva

2000 Povelja Evropske unije o osnovnim pravima

2002, 2006, 2009 Direktiva o privatnosti i elektronskim komunikacijama

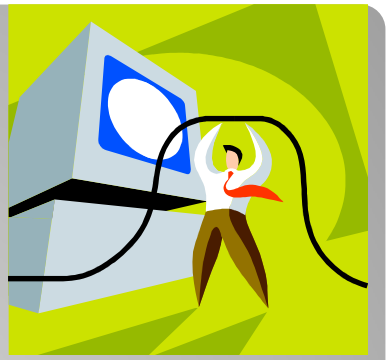
GDPR-Cilj

- sprečavanje i ograničavanje neadekvatne razmene i skladištenja ličnih podataka korisnika
- globalni standard za upravljanje podacima - efikasnije upravljati podacima o svojim kupcima, zaposlenima, kontaktima i svim drugim relevantnim osobama
- harmonizacija prava
- odgovornost kompanija kazne 2% do 4% godišnjeg prometa ili 10-20 miliona evra
- obaveza obaveštavanja o gubitku podataka u roku od 72h
- potrebne procene uticaja na privatnost

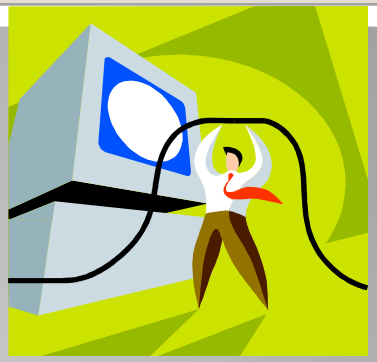


O GDPR-Poglavlja

- I-Opšte odredbe
- II-Načela
- III-Prava lica na koje se podaci odnose
- IV-Rukovodilac i obrađivač podataka
- V-Prenosi podataka o ličnosti trećim zemljama ili međunarodnim organizacijama
- VI-Nezavisni nadzorni organ
- VII-Saradnja i konzistentnost
- VIII-Pravna sredstva, odgovornost i sankcije
- IX-Odredbe u vezi sa posebnim situacijama obrade
- X-Delegirani akti i akti za sprovođenje
- XI-Završne odredbe



O GDPR



Doneta 27. aprila 2016.

Uredba o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka i o stavljanju van snage Direktive 95/46/EZ

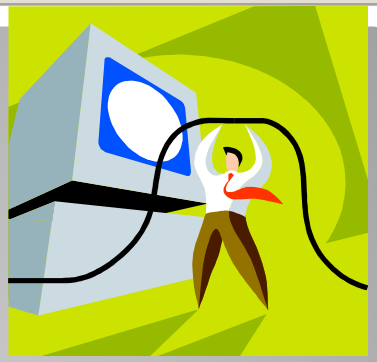
99 članova podeljenih u 11 poglavlja

Primenjuje se od 25. maja 2018.

GDPR zahteva:

evidenciju, saglasnost, obaveštenja, nova prava, privatnost, bezbednost, odgovor na incidente, i prenos podataka

GDPR-na koga se odnosi



Lice čiji se podaci prikupljaju i obrađuju (Data Subject)

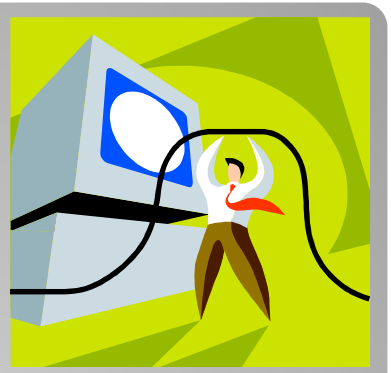
Odgovorno lice - rukovalac (Data Controller) - analizira relevantne tehničke i organizacione mere posebno u pogledu zaštite informacija, sigurnosti informacija i odgovora na incidente, prati i dokumentuje primenu i efikasnost svojih politika

Obrađivač podatak (Data Processor)

Službenik za zaštitu podataka (Data Protection Officer)- informiše i savetuje odgovorno lice podataka ili obrađivača, kao i zaposlene, prati usaglašenost sa zakonima o zaštiti podataka, sarađuje i deluje kao kontakt osoba za nadzorne organe

Organ za zaštitu podataka – Poverenik (Data Protection Authoriti)

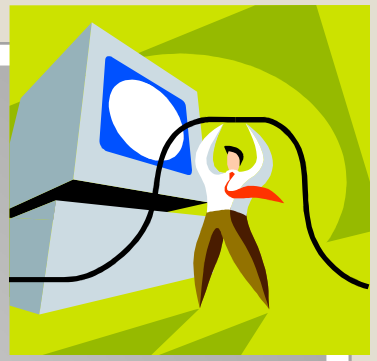
GDPR- na koga se primenjuje



Primjenjuje se na rukovaoce i obrađivače koje obrađuju lične podatke, a imaju sedište u EU (čl. 3. GDPR)

Primjenjuje se na rukovaoce i obrađivače koje obrađuju lične podatke koji NEMAJU sedište u EU a) ako nude robu ili usluge građanima EU ili b) prate ponašanje građana EU (čl. 3. GDPR)

GDPR-Prava lica čiji se podaci prikupljaju i obrađuju



Pravo na informisanje

Pravo na zaborav, brisanje

Pravo na prenosivost podataka

Pravo na ograničenje

Pravo na ispravku

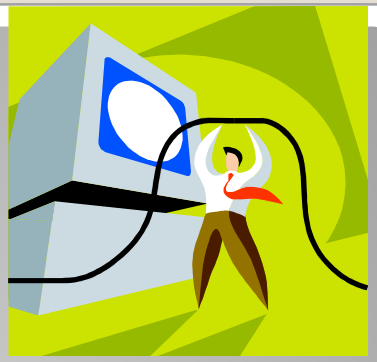
Pravo pristupa ličnim podacima

Pravo na prigovor

Pravo da se spreči automatska obrada, uključujući profilisanje (obrada samo uz jasnu nedvosmislenu saglasnost)

Pravo na obaveštavanje o zloupotrebama

Evidencija o aktivnostima obrade ličnih podataka



Obaveza vođenja evidencija o procesima obrade:

Identifikacija odgovornih lica / obrađivača /službenika/

Svrha obrade

Opis prikupljenih obrađenih podataka - identifikacija lica o kojima se prikupljaju podaci

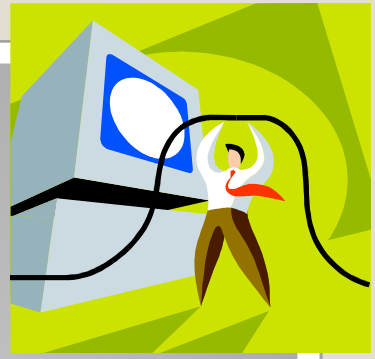
Primaoci

Transferi

Vremenski rok za brisanje

Tehničke i organizacione mere sigurnosti

Obaveštenja za lica čiji se podaci prikupljaju i obrađuju



Identitet službenika za zaštitu podataka

Svrha prikupljanja

Period čuvanja

Pravo pristupa, ispravke, ograničenja i prigovora

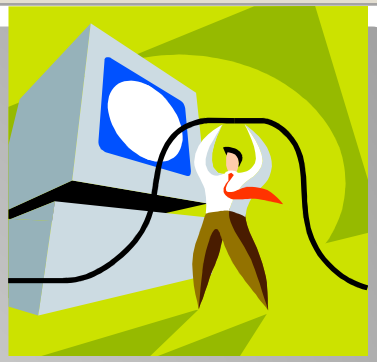
Pravo da podnesu žalbu

Pravo povlačenja saglasnosti u bilo koje vrijeme

Informacije o profiliranju

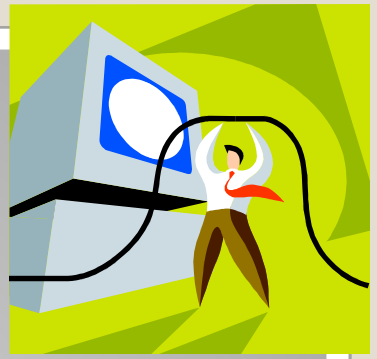
Sve druge informacije koje garantuju sigurnost i zakonitost obrade

Saglasnost lica čiji se podaci prikupljaju i obrađuju



- Nova definicija saglasnosti koja zahteva jasnu afirmativnu akciju
- Nove smernice u vezi s "slobodno datim" pristankom
- Nove okolnosti u kojima je potrebna izričita saglasnost
- Saglasnost maloletnika

Saglasnost
Primer usaglašenosti sa GDPR



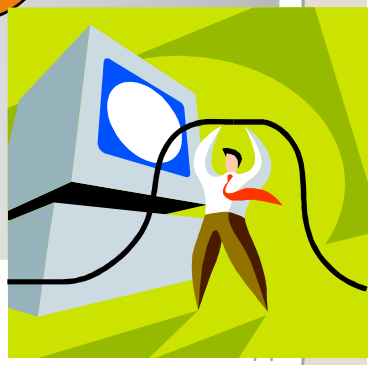
-Ako pojedinac **povuče saglasnost ili podnese prigovor** na ono što radite sa njegovim podacima, da li možete odmah prekinuti obradu tih podataka? (Čl. 21. GDPR)

Nivo 0	Nivo 1	Nivo 2
Ne	Osim ako to nije preterano teško, u nekim slučajevima ćemo poštovati takve primedbe	Da, obaveštavamo ljude o njihovom pravu na prigovor, pružamo im sredstva za to, i mi smo u stanju da prekinemo obradu tih podataka

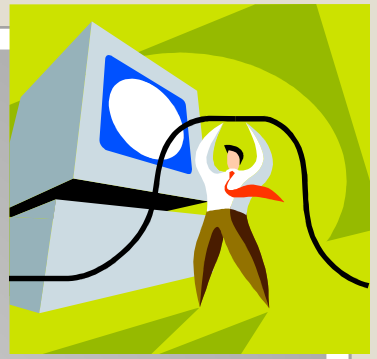
Bezbednost - pseudonimizacija

-GDPR – definicija

„pseudonimizacija” je obrada podataka o ličnosti na takav način da podaci o ličnosti više ne mogu da se povežu s konkretnim licem na koje se podaci odnose bez korišćenja dodatnih informacija, pod uslovom da se takve dodatne informacije čuvaju odvojeno i da se na njih primenjuju tehničke i organizacione mere da bi se obezbedilo da podaci o ličnosti ne mogu da se povežu s fizičkim licem čiji je identitet određen ili se može odrediti



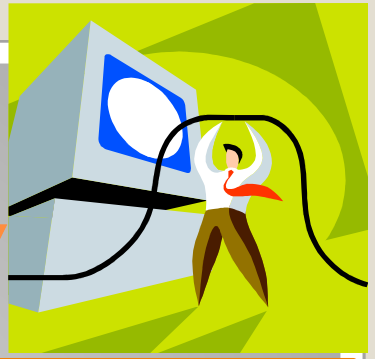
Bezbednost
Primer usaglašenosti sa GDPR



-Bezbednost obrade podrazumeva pseudonimizaciju i enkripciju (čl. 32 stav 1. GDPR)

Nivo 0	Nivo 1	Nivo 2
Ne koristi se	Koristi se u nekim delovima obrade podataka	Koristi se uvek, odnosno kad god je to moguće

Odgovor na incident "curenje"

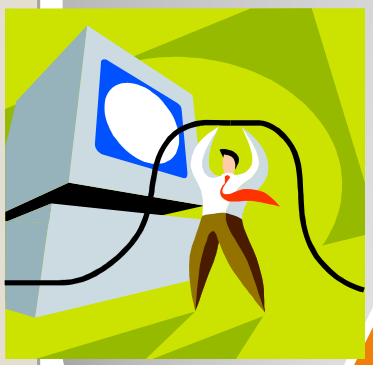


povreda bezbednosti koja dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmene, neovlašćenog otkrivanja ili pristupa ličnim podacima koji se šalju, čuvaju ili na drugi način obrađuju

bilo koji incident koji utiče na poverljivost, integritet, dostupnost, provera adekvatnost mera bezbednosti

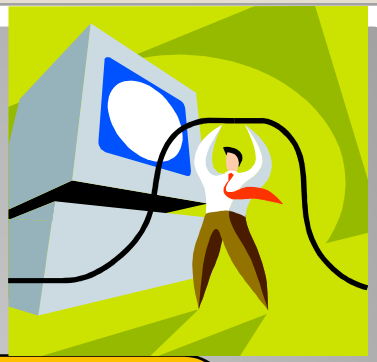
vrsta incidenta, obaveštavanje u roku od 72h, posledice, preduzete mere, obaveštenje bez nepotrebnog odlaganja u slučaju visokog rizika za prava i slobodu pojedinaca, nema obaveštenja ako su podaci šifrirani, ukoliko su preduzete tehničke mere ili ako obaveštenje podrazumeva nesrazmerne napore (Čl. 33 i 34 GDPR)

GDPR – Posledice za kompanije



1. Pripremiti evidenciju aktivnosti obrade
2. Uspostaviti globalnu politiku za zaštitu podataka i upravljanje
3. Potvrditi rešenje za prekogranično prebacivanje podataka
4. Ažurirati svoj globalni plan obaveštenja o "curenju" podataka
5. Pripremiti obaveštenja za korisnike
6. Obezbediti obaveštenja vlasnicima informacija
7. Obaveze obrađivača podataka
8. Imenovanje službenika za zaštitu podataka
9. Razmotriti novčane kazne i posledice

Kazne i posledice



-10M EURA 2% ukupnog godišnjeg prometa u prethodnoj finansijskoj godini. PRIMER: Za neadekvatne sisteme / procese, "minorno" kršenje (Čl. 83. GDPR)

-20M EURA 4% ukupnog godišnjeg prometa u prethodnoj finansijskoj godini. PRIMER: Kršenje osnovnih principa za obradu, za prenos podataka na daljinu, velike povrede podataka, eksploataciju podataka (Čl. 83. GDPR)

HVALA NA PAŽNJI