

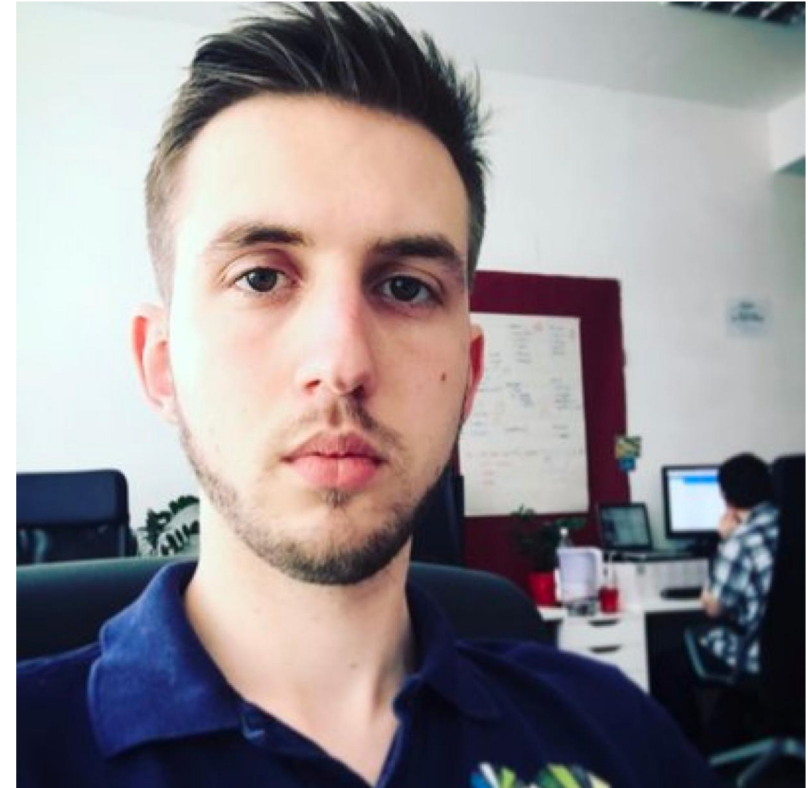
Zálohy vs. GDPR

Marek Galinski, Ján Golais



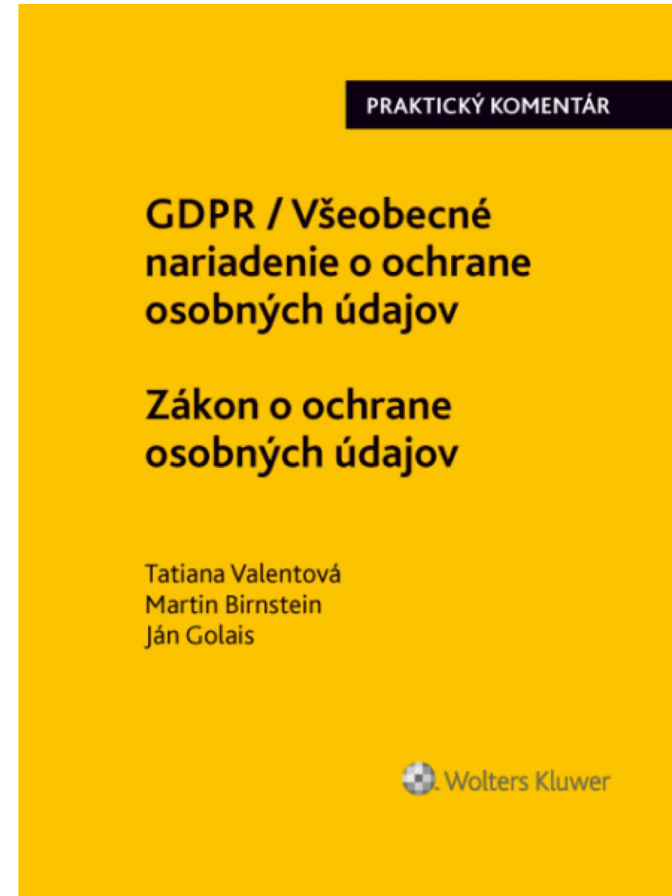
O Autoroch

- Marek Galinski
 - PhD študent @ FIIT STU Bratislava
 - CEO Regex s.r.o.
 - Organizátor Bratislava OpenCamp



O Autoroch

- Ján Golais
 - Mgr. PRAF UK Bratislava
 - Data Privacy Advisor @ Telekom
 - Spoluautor komentára k
Zákonu o ochrane osobných údajov
18/2018 Z.z.



Prečo vzniklo GDPR?

- Potreba aby v dobe, kedy už nikto nemá prehľad o tom a ako spracováva naše osobne údaje, existoval jednotný predpis záväzný pre celý EHP, ktorý vráti občanom možnosť kontrolovať a rozhodovať o tom, ako sa narába s ich osobnými údajmi.



Prečo vzniklo GDPR?

- Posilňuje prevenciu
 - Podmienenie spracúvania osobných údajov vedomým a preukázateľným súhlasom dotknutej osoby
 - Obmedzenie rozsahu spracúvaných osobných údajov
 - Objasňuje dotknutým osobám ich práva



Prečo vzniklo GDPR?

- Núti prevádzkovateľov rozmýšľať
 - Prevádzkovateľ musí mať jasno ako a aké dáta spracúva
 - Kladie nároky na bezpečnosť osobných údajov v informačnom systéme



Vecná pôsobnosť

- Vztahuje sa na spracúvanie osobných údajov úplne alebo čiastočne automatizovanými prostriedkami, alebo inými než automatizovanými prostriedkami, ak sú určené na to, aby tvorili súčasť informačného systému.



Vecná pôsobnosť

- Nevzťahuje sa na spracúvanie osobných údajov fyzickou osobou výlučne osobnej alebo domácej činnosti.
 - súkromná korešpondencia
 - geolokalizácia v rámci rodiny
 - domáci kamerový systém, ak nesníma verejný priestor



Vecná pôsobnosť

- Nevzťahuje sa na spracúvanie osobných údajov Slovenskou informačnou službou alebo Vojenským spravodajstvom.



Osobný údaj

- Informácia týkajúca sa identifikovanej, alebo identifikovateľnej fyzickej osoby, pričom je identifikovateľná priamo alebo nepriamo
 - meno, identifikačné číslo, lokalizačný údaj, online identifikátor
 - odkaz na fyzický, fyziologický, genetický, mentálny, ekonomický, kultúrny alebo sociálny prvok špecifický pre identitu fyzickej osoby



Spracúvanie

- Operácia alebo súbor operácií s osobnými údajmi
 - získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom alebo šírením, preskupovanie, kombinovanie, obmedzenie, vymazanie, likvidácia
 - bez ohľadu na to, či sa vykonávajú automatizovanými prostriedkami alebo nie



Lokálna legislatíva

- Slovenská republika
 - Zákon č. 18/2018 Z.z. z 29. novembra 2017 o ochrane osobných údajov
 - Účinný od 25.5.2018
- Česká republika
 - Nařízení Evropského parlamentu a Rady [EU] 2016/679 ze dne 27. dubna 2016
 - Nahradilo zákon č. 101/2000 Sb., o ochraně osobních údajů dňa 25. 5. 2018



Čo nastalo s príchodom GDPR?



Čo nastalo s príchodom GDPR?



Čo nastalo s príchodom GDPR?



1 of 2



Toto nemusí byť Váš posledný e-mail z SND.  Inbox x



SND newsletter@snd.sk via se-bounce-0001.cz
to me ▾

Thu 24 May, 18:45



**Mení sa zákon.
Bud'te aj naďalej prví,
ktorí sa dozvedia
o tom, čo sa deje
v SND.**



Čo nastalo s príchodom GDPR?

The International Association of Privacy Professionals
predpovedá vznik najmenej 75,000 pracovných miest a
spoločnosti Fortune's Global 500 companies minú 8 miliárd
dolárov na vypracovanie GDPR politik

Práva dotknutej osoby

- Právo na prístup k osobným údajom
- Právo na opravu osobných údajov
- Právo na obmedzenie spracúvania
- Právo na vymazanie osobných údajov



Práva dotknutej osoby

- Právo na prístup k osobným údajom
- Právo na opravu osobných údajov
- Právo na obmedzenie spracúvania
- Právo na vymazanie osobných údajov



Konflikt

Právo na vymazanie
osobných údajov

vs.

Technické možnosti a
obmedzenia
prevádzkovateľa systému

Právo na vymazanie osobných údajov

- [1] Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.
- [2] Prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak dotknutá osoba uplatnila právo na výmaz podľa odseku 1, ak
 - a) osobné údaje už nie sú potrebné na účel, na ktorý sa získali alebo inak spracúvali,
 - b) dotknutá **osoba odvolá súhlas** podľa § 13 ods. 1 písm. a) alebo § 16 ods. 2 písm. a), na základe ktorého sa spracúvanie osobných údajov vykonáva, a neexistuje iný právny základ pre spracúvanie osobných údajov,
 - c) ...
 - d) osobné údaje sa spracúvajú nezákonne,
 - e), f), ...



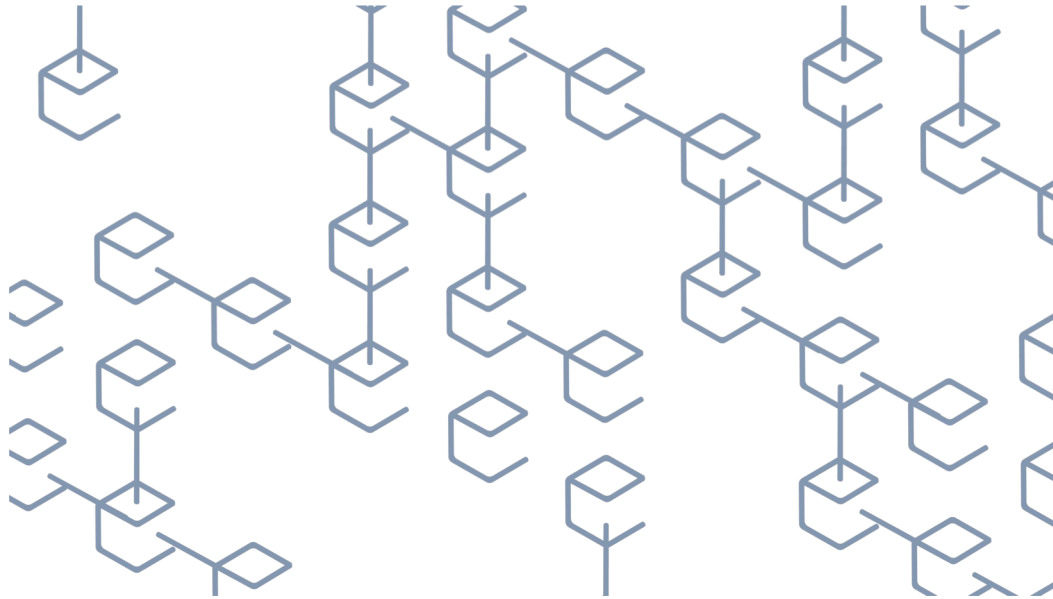
Právo na vymazanie osobných údajov

- A čo má prevádzkovateľ urobiť so zálohami?



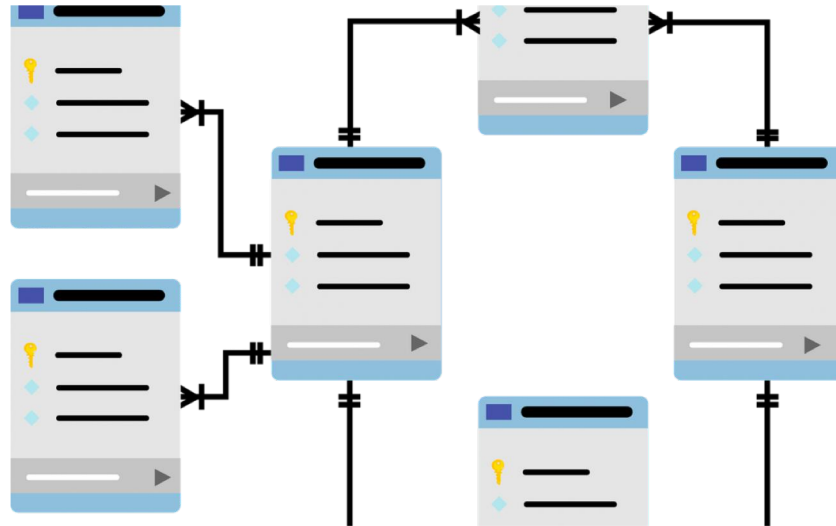
Právo na vymazanie osobných údajov

- A čo má prevádzkovateľ urobiť s blockchainom?



Právo na vymazanie osobných údajov

- A čo má prevádzkovateľ urobiť s relačnými databázami?



Najčastejšie chybné argumenty

- „Je to iba v zálohách a samotné údaje sa nijak nespracúvajú...”
 - Aj uchovávanie sa na účely predpisu rozumie ako spracúvanie
- „Nevedeli sme, že tie dáta v nejakých zálohách máme...”
 - Pán policajt, neviem ako rýchlo som išiel, takže mi nemôžte dať pokutu

Najčastejšie chybné argumenty

- „Náš systém neumožňuje takéto zmazanie údajov“

§ 31 Prevádzkovateľ

[1] S ohľadom na povahu, rozsah a účel spracúvania osobných údajov ... je prevádzkovateľ povinný **prijatť vhodné technické a organizačné opatrenia** na zabezpečenie a preukázanie toho, že spracúvanie osobných údajov sa vykonáva v súlade s týmto zákonom.

Ako na to?

- Ako teda uspokojiť požiadavky GDPR a uplatniť dotknutej osobe právo na vymazanie [right to be forgotten]?
 - Právne možnosti
 - Technické možnosti



Právne možnosti

- Nájsť si zákonný dôvod, prečo dáta uchovávať

[4] Odseky 1 a 2 sa neuplatňujú, ak je spracúvanie osobných údajov potrebné

a) na uplatnenie práva na slobodu prejavu alebo práva na informácie,

b) na splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,

c), d), e) ...



Právne možnosti

Pokiaľ sú vaše osobné údaje spracúvané v rámci plnenia zákonnej povinnosti Tatra banky, príslušné právne predpisy bližšie určujú dobu, počas ktorej je Tatra banka povinná vaše osobné údaje a súvisiacu dokumentáciu uchovávať.

Zákon o kolektívnom investovaní, ktorý v § 55 ods. 5 stanovuje povinnosť uchovávať identifikačné údaje alebo kópie dokladov o preukázaní totožnosti investorov a klientov a doklady o zisťovaní vlastníctva prostriedkov použitých investormi a klientmi na vykonanie obchodu **aspoň desať rokov od ukončenia obchodu.**

Pravidlá spracúvania osobných údajov, Tatra Banka, a.s.



Právne možnosti

Alumni účely - Oprávnený záujem [čl. 6 ods. 1 písm. f) GDPR]:
udržiavanie kontaktu s absolventami

Pravidlá spracúvania osobných údajov,
Slovenská Technická Univerzita v Bratislave



Právne možnosti

Športový zväz v SR - Oprávnený záujem [čl. 6 ods. 1 písm. f) GDPR]:
historické a štatistické údaje o hráčoch.



Právne možnosti

We will keep your information for as long as we need it for the purpose it is being processed for. For example, where you book a flight with us we will keep the information ... so we can fulfil the specific travel arrangements you have made and after that, we will keep the information for a period which enables us to handle ... complaints ... relating to the booking.

If you stop interacting with us as a customer, we will remove or anonymise your information after 7 years.

British Airways Privacy Policy



Technické možnosti

- Automatizovaný mechanizmus premazávania
- Informácia o zneplatnení údajov
- Pseudonymizácia / anonymizácia dát
- Oddelenie citlivých dát od necitlivých
- Oddelené zálohovanie



Automatizovaný mechanizmus mazania

- Každý údaj má svoju expiračnú značku – tzn. informáciu o tom, dokedy musí byť uchovávaný.
- Automatizovaný skript periodicky premazáva nepotrebné údaje.
- Pri obnovení zálohy po incidente pred nasadením dát do produkcie skript prejde zálohy a odstráni to, čo obnovené byť nemá.



Automatizovaný mechanizmus mazania

- Ak uchováвате zálohy iba určité časové obdobie, napr. 1 mesiac, požiadavka je *de facto* naplnená.
- Pri žiadosti o výmaz sa údaje vymažú z produkčných databáz a zvyšné zaniknú po 30 dňoch samé.



Automatizovaný mechanizmus mazania

Keďže zálohy môžu obsahovať osobné údaje [napríklad dumpy databáz] dbáme na ich bezpečnosť. Zálohy sú automaticky mazané po 14 dňoch a snapshoty [VPS a VDC] po 28 dňoch – takže v prípade požiadavky „práva za zabudnutie“ je naplnená takýmto spôsobom.

Pravidlá ochrany osobných údajov
WebSupport.sk



Informácia o zneplatnení údajov

- Ak údaje zo záloh nie je možné priamočiaro odstrániť, treba mať mechanizmus, ktorý predchádza obnove týchto údajov.
- Pseudonymizovaná informácia o tom, ktoré dáta treba pri obnove odstrániť.
 - Napr. zoznam nič nehovoriacich *userID*.



Pseudonymizácia a anonymizácia dát

- Ak sú údaje zálohované a dlhodobo uchovávané pre možnosť spätne ich obnoviť, treba ich pseudonymizovať, tzn. zálohovať údaje tak, aby dotknuté osoby mohli byť stotožnené iba použitím iných údajov.
 - Používať nič nehovoriaci identifikátor tak, aby citlivé údaje boli len na jednom jedinom mieste, odkiaľ je jednoduché ich odstrániť.



Pseudonymizácia a anonymizácia dát

- Ak sú údaje zálohované a dlhodobo uchovávané pre štatistické účely, riešením je ich anonymizácia.
 - Tzn. znemožnenie spätného stotožnenia jednotlivých údajov s konkrétnou fyzickou osobou.



Oddelenie citlivých a necitlivých údajov

- Ak je to možné, treba držať citlivé dáta vždy oddelene, tak aby bolo jednoduché ich odstrániť bez nutnosti prechádzať veľké množstvo dát.
 - Pozor pri noSQL databázach
 - Pozor na *foreign keys* v relačných databázach



Oddelenie záloh

- Zálohy citlivých dát mať po ruke pre potrebu uspokojiť požiadavku na vymazanie dát.
- Zálohy necitlivých dát mať tým pádom „na háku“.



Blockchain a logy

- Nikdy nedávať identifikovateľné údaje do blockchainu alebo do logov.
- Používať pseudo-identifikátor aby po vymazaní informácie o tom, komu identifikátor patrí boli dáta v logoch / blockchaine nestotožniteľné.



Google Analytics a GDPR

- Zapnite anonymizáciu IP adries a nezabudnite na vaše podmienky spracúvania osobných údajov.



The screenshot shows the Google Analytics configuration interface. At the top, the 'Tracking ID' is set to 'UA-99999-9'. Below it, the 'Cookie Domain' is set to 'auto'. A section titled 'More Settings' is expanded, showing 'Fields to Set'. In this section, the 'Field Name' is 'anonymizelp' and the 'Value' is 'true', indicating that IP anonymization is enabled. There are plus and minus icons next to the field name and value inputs, and a minus icon at the end of the row.

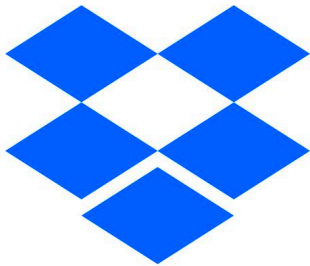
Field Name	Value
anonymizelp	true



Zálohy tretích strán



Google Drive



Zálohy tretích strán

- Ak dáta o vašich používateľov odovzdávate tretím stranám [Google, MS Azure, Dropbox, ...] zistite si, ako oni aplikujú požiadavku na uplatnenie práva byť zabudnutý.
- Služby dnes na tento účel poskytujú spravidla nejaké API.
- Mnohé prípady vyžadujú „manual file submission“.



Zálohy tretích strán

- Vy ste spoluzodpovední za prípadne prešlapy tretích strán.

§ 33 Spoloční prevádzkovatelia

[1] Spoločnými prevádzkovateľmi sú dvaja prevádzkovatelia alebo viacerí prevádzkovatelia, ktorí si dohodou určia účel a prostriedky spracúvania osobných údajov. V dohode sú zároveň povinní transparentne určiť zodpovednosť každého z nich za plnenie povinností a úloh podľa tohto zákona, V dohode sa tiež určí kontaktné miesto pre dotknutú osobu.

[3] Bez ohľadu na podmienky dohody podľa odseku 1 môže dotknutá osoba uplatniť svoje práva u každého prevádzkovateľa a voči každému prevádzkovateľovi.



Rady na záver – čo robiť?

- Majte prehľadné podmienky spracúvania osobných údajov
 - Vysvetlite v podmienkach jasne aké údaje, na aké účely a ako dlho spracúvate.
 - Vysvetlite fungovanie vašich záloh – ako a prečo?
 - Vysvetlite používateľovi ako si môže uplatniť svoje práva.
 - Budte transparentní voči používateľovi.



Rady na záver – čo robiť?

- Zabezpečte, aby vymazaný používateľ o vás už nikdy nepočul
 - Dbajte najmä na marketingové databázy a mailing listy
 - Zamedzte možnosti, aby používateľ, ktorý požiadal o zmazanie, bol obnovený do marketingovej alebo mailovej databázy



Rady na záver – čo robiť?

- Iba potrebné osobné údaje, iba potrebný čas
 - Neukladajte a nezálohujte osobné údaje, ktoré nevyhnutne nepotrebuje.
 - Neukladajte údaje dlhšie, než ich nevyhnutne potrebujete.



Rady na záver – čo robiť?

- Majte jasné procesy obnovovania zálohovaných údajov
 - Predchádzajte tomu, aby sa obnovou zo zálohy do produkčného systému vrátili údaje používateľa, ktorý medzičasom odvolal súhlas alebo požiadal o výmaz.



Rady na záver – čo robiť?

- Budte pripravení rýchlo zmazať osobné údaje z produkčnej inštalácie a horúcej zálohy.
 - Majte mechanizmus, ktorým napr. rýchlo a účinne [ideálne okamžite] odstránite používateľove dáta z mailing listov, verejných databáz, etc.
 - Pozor na ľudský faktor



Rady na záver – čo robiť?

- Ak dáta zo záloh nemôžete mazať, vysvetlite prečo.
 - Poskytnite používateľovi jasné vysvetlenie, prečo sú jeho údaje vo vašom systéme a vašich zálohách.



Rady na záver – čo robiť?

- Znemožnite zneužitie záloh.
 - Šifrovanie záloh
 - Pseudonymizácia záloh
 - Anonymizácia záloh
 - Fyzická bezpečnosť záloh



Rady na záver – čo robiť?

- Nikdy nepoužiť osobné údaje na niečo, na čo ste nedostali súhlas dotknutej osoby
 - Dôvera medzi vami a používateľom vyrieši veľa potenciálnych problémov.

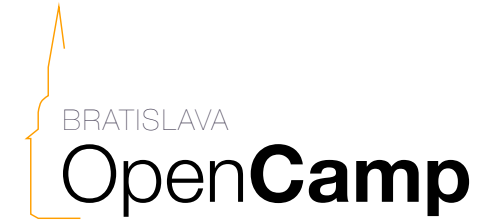


Rady na záver – čo robiť?

- Nepanikáriť.



Bratislava OpenCamp 2019



13.4.2019

FIIT STU, Bratislava

- Call for Papers
- Call for Partners
- www.opencamp.sk



Otázky?

