



Zmeny nevyhnutné pri príprave na GDPR
15. marec 2018

Peter Bíro (CEO)

Obsah seminára

1. Nariadenie GDPR a jeho požiadavky
2. GDPR z pohľadu registra voči registrátorovi (registrátorská zmluva a postupy)
3. GDPR z pohľadu registrátora voči držiteľovi (prenesené podmienky)
4. GDPR z pohľadu registrovania domén (I. nastavenie Pravidiel, II. ďalšia legislatíva)

14:00 – 16:00





1: Nariadenie GDPR a jeho požiadavky





GDPR

Nariadenie GDPR a jeho požiadavky (1/5)

- **25. máj 2018** = účinnosť
- Nariadenie = priamo + zákon č. 18/2018 – pokuta do 20 mil. / 4% obratu
- Osobné údaje – akékoľvek informácie o priamo alebo nepriamo identifikovateľnej FO (=dotknutá osoba)
- Informačný systém – akýkoľvek súbor OÚ dostupný podľa kritérií, nezávisle či centralizovaný / necentralizovaný / distribuovaný (nielen e- !)
- Prevádzkovateľ = kto určuje účely a prostriedky spracúvania OÚ (priamo/ podľa zákona)
- Sprostredkovateľ = spracúva OÚ v mene prevádzkovateľa
- Vzťahuje sa ak je prevádzkovateľ/sprostredkovateľ z EÚ alebo dotknuté osoby sú z EÚ (tovary & služby)

Nariadenie GDPR a jeho požiadavky (2/5)

- Primerané a minimalizované spracúvanie na výslovne uvedený legitímny účel, správne a podľa potreby aktualizované OÚ, minimalizácia uchovávaní, integrita a dôvernoscť, preukázanie súladu (zodpovednosť) **(čl. 5)**
- Zákonncé spracúvanie – súhlas / zmluva / zákon / životné záujmy / verejný záujem / oprávnené záujmy **(čl. 6)**
- Osobitné kategórie OÚ – zdravie / biometria / politika / náboženstvo... nie RČ **(čl. 9)**
- Už nie bezp. projekt, ale primerané technické a organizačné opatrenia na ochranu **(čl. 24, 25, 28)**

Nariadenie GDPR a jeho požiadavky (3/5)

➤ Práva dotknutej osoby:

- Právo na údaje (či sú + ich získať) **(čl. 15)** – žiadny nepriaznivý vplyv na práva iných!
- Práva s oznamovacou povinnosťou (okrem pri neprimeranom úsilí): **(čl. 19)**
 - Právo na opravu **(čl. 16)**
 - Právo na vymazanie (za určitých podmienok) **(čl. 17)**
 - Právo na obmedzenie spracúvania **(čl. 18)** + právo namietat spracúvanie **(čl. 21)**
- Právo na prenosnosť **(čl. 20)**
- Právo vylúčiť sa z automatizovanej kategorizácie (vrátane profilovania) **(čl. 22)**

Nariadenie GDPR a jeho požiadavky (4/5)

- Zodpovedná osoba = DPO (**oddiel 4, čl. 37+**) – aj externá / spoločná – oznámiť ÚOOÚ!
- Kódexy správania – zástupcovia kategórií prevádzkovateľov / sprostredkovateľov – schvaľuje ÚOOÚ (ak viac ČŠ, tak EK) (**oddiel 5, čl. 40+**)
 - v SR zatiaľ neexistuje
- Akreditácia subjektu pre monitorovanie súladu s kódexom (certifikačné subjekty) -> dobrovoľná certifikácia prevádzkovateľov / sprostredkovateľov – neznižuje zodpovednosť! (**čl. 42+**)
 - v SR zatiaľ neexistuje

Nariadenie GDPR a jeho požiadavky (5/5)

- Podporná dokumentácia rozhodnutiam a nastaveniam = procesné analýzy, bezpečnostné a organizačné opatrenia atď.!
- Konzultovať s DPA (ÚOOÚ)
- Princíp – urobiť čo najviac a veriť, že to bude stačiť





2: GDPR z pohľadu registra voči registrátorovi



GDPR z pohľadu registra voči registrátorovi (1/3)

- Registrátor je sprostredkovateľ **(čl. 28)** a v rámci svojich vlastných činností zároveň nezávislý prevádzkovateľ **(čl. 24)**
- Zmluvný základ – vo forme dodatku – nepodpísanie = podstatné porušenie zmluvy
- Podpisovanie od schválenia Pravidiel Komisiou (od ~6. apríla) do 24.5.2018
- Obsahuje povinné zmluvné podmienky **(čl. 29. ods. 3)**, v SR nie sú prijaté tzv. štandardné zmluvné doložky
 - Účel spracúvania, rozsah **(3.)**

GDPR z pohľadu registra voči registrátorovi (2/3)

- Bezpečnosť + mlčanlivosť (= opatrenia na zabránenie neoprávnenému spracúvaniu, t.j. dôvernosti a integrity) **(4.) (najmä z čl. 28, ods. 3 b))**
- Súčinnosť + povinnosti priamo definované v GDPR **(5.)**
 - Povinné bezodkladné oznámenie porušenia ochrany OÚ (SK-NIC následne do 78h, ak môže viesť k rizikám pre práva a slobody FO + za určitých okolností aj dotknutej osobe)
 - Obsah: Opis porušenia, aké kategórie, koľko osôb, kontaktná osoba, dopad, prijaté opatrenia (vzor v príprave)
- Subdodávateľia (prenesenie záväzku) **(6.)**

GDPR z pohľadu registra voči registrátorovi (3/3)

- Kontrolné právomoci (7.) = audits, iniciatívne oznámenie porušovania (z čl. 28, ods. 3 h))
- Prenos OÚ do tretích krajín (8.) – súhlas so spracúvaním v Eur. združení voľného obchodu (Švajčiarsko, UK po Brexite) za splnenia GDPR
- Doba trvania spracúvania (počas zmluvy + zákonné podmienky) (9.)
- Povinný výmaz (z čl. 28, ods. 3 g)) (10.)
- Platnosť podpisom, účinnosť 25.5.2018



3: GDPR z pohľadu registrátora voči držiteľovi



GDPR z pohľadu registrátora voči držiteľovi (1/2)

- Register: Zmluvný základ voči používateľovi (aj pri záujme o reg.), súhlas pri WHOIS
- Registrátor: Povinná zmluva s držiteľom (**9.17 Pravidiel** „Zmluvné vzťahy medzi Registrátorom a Používateľom sa riadia príslušnou zmluvou medzi nimi...”)
- Poskytnutie informácie používateľovi (**čl. 12 transparentnosť**) + evidencia poskytnutia Pravidiel
- **9.6.9 Pravidiel**: „zabezpečiť a zdokumentovať, že každý Používateľ, ktorému Registrátor registruje kontaktné údaje súhlasil s dodržiavaním Pravidiel a podmienkami týkajúcimi sa ochrany osobných údajov podľa Pravidiel, a to najneskôr pri príslušnej registrácii“

GDPR z pohľadu registrátora voči držiteľovi (2/2)

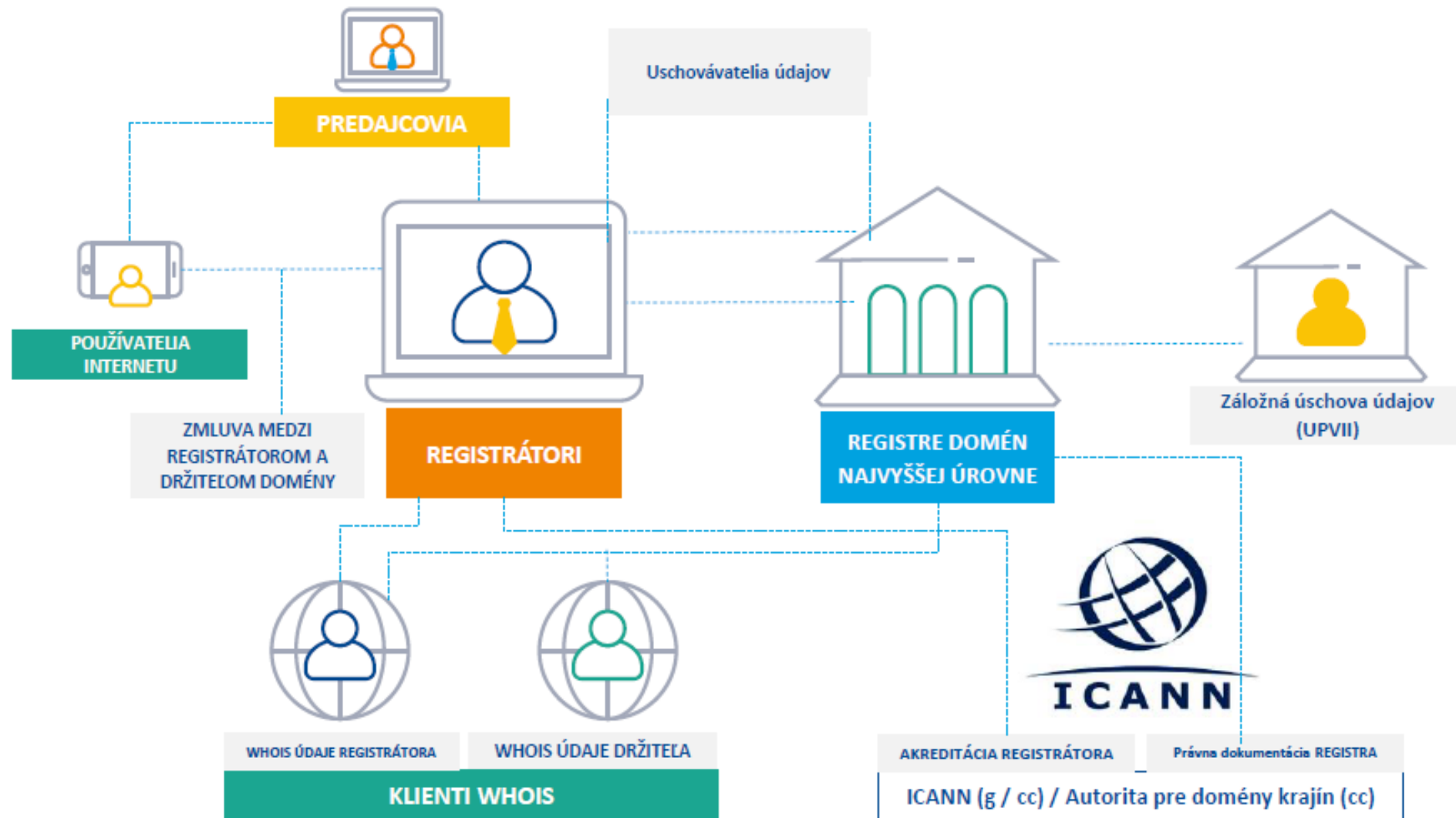
- Zistenie veku (16+) + evidencia / preukaznosť súhlasu v prípade záujmu o zverejňovanie vo WHOIS
- Údaje: Meno, priezvisko, bydlisko (doručovací adres), e-mail + telefón, dátum narodenia +
 - register môže dopýtať ďalšie, registrátor má navyše min. finančné údaje)
 - kontaktné údaje držiteľa typu právnická osoba môžu byť osobné údaje
 - IP adresa = OÚ
- Právo na prenosnosť **(čl. 20)**



4: GDPR z pohľadu registrovania domén



GDPR z pohľadu registrovania domén (1/7)



GDPR z pohľadu registrovania domén (2/7)



INFORMÁCIE O DOMÉNE

Doména:	tld.sk
Držiteľ:	EURO-0001
Admin. kontakt:	EURO-0001
Technický kontakt:	EURO-0001
Registrátor:	EURO-0001
Dátum vytvorenia:	2003-06-10
Posledná zmena:	2017-09-01
Platná do:	2018-06-10
Menný server:	a.tld.sk
Menný server:	c.tld.sk
Menný server:	sns-pb.isc.org
Menný server:	b.tld.sk
EPP Status:	ok

KONTAKTNÉ ÚDAJE DRŽITEĽA DOMÉNY

Kontakt:	JOZM-0003
Názov:	Jozef Mrkvička
Telefón:	+421.566683770
Email:	hostmaster@sk-nic.sk
Ulica:	Kollárova 6
Obec:	Bratislava
PSČ:	85101
Kód štátu:	SK
Registrátor:	SK-NIC
Dátum vytvorenia:	2017-09-01
Posledná zmena:	2017-09-01

KONTAKTNÉ ÚDAJE REGISTRÁTORA

Registrátor:	SK-NIC
Organizácia:	SK-NIC, a.s.
IČO:	35698446
Telefón:	+421.235035030
Email:	hostmaster@sk-nic.sk
Webové sídlo:	www.sk-nic.sk
Ulica:	Borská 6
Obec:	Bratislava
PSČ:	84104
Kód štátu:	SK
Dátum vytvorenia:	2017-09-01
Posledná zmena:	2018-02-12

ADMINISTRATÍVNY / TECHNICKÝ KONTAKT

Kontakt:	JOZM-0003
Názov:	Jozef Mrkvička
Telefón:	+421.566683770
Email:	hostmaster@sk-nic.sk
Ulica:	Kollárova 6
Obec:	Bratislava
PSČ:	85101
Kód štátu:	SK
Registrátor:	SK-NIC
Dátum vytvorenia:	2017-09-01
Posledná zmena:	2017-09-01

GDPR z pohľadu registrovania domén (3/7)



- Zmena Pravidiel + dodatok k registrátorskej zmluve
- Proces:
- Verejné pripomienkovanie zmien: **9. – 21.3.2018**
- Stretnutie Komisie: **5.4.2018**
- Podpisovanie dodatku: **~6.4. – 24.5. 2018**
- Finále = **25.5.2018**



GDPR z pohľadu registrovania domén (4/7)



- Účely spracúvania: **(8.8 Pravidiel)**
 - Evidencia Používateľa v Registri a súvisiace uzatvorenie zmlúv
 - Poskytnutie OÚ osobe s preukázaným oprávneným záujmom (napr. advokáti)
 - Poskytnutie OÚ Centru ADR
 - Spracúvanie údajov nad rámec minima ak ich Používateľ poskytol pre komunikáciu a jednoznačnú identifikáciu
 - Vytváranie zálohy zónového súboru podľa zmluvy so štátom
 - Zverejnenie prostredníctvom osobitnej služby na zverejňovanie (napr. WHOIS, RDAP...)
- Minimum: meno, priezvisko, adresa (bydlisko / doručovacia), e-mail **(8.2.6 Pravidiel)**
- Návrh počíta s možnosťou budúcej voľby zverejniť skryté (prednastavené všetko skryté)
- Spracovanie 6 mesiacov (oprávnené záujmy používateľa) + zákonné lehoty (napr. trestný zákon)

GDPR z pohľadu registrovania domén (5/7)



- Prenos do tretích krajín na základe povolenia registrom **(8.6 Pravidiel)**
- 16- rokov môže byť, ale pri súhlase (WHOIS) doklad zákonného zástupcu **(8.7 Pravidiel)**
- Ostatné – povinné informácie (práva, kontakty, kam sťažnosti) **(8.8+ Pravidiel)**
- Odstránenie mena a priezviska pri FO z WHOIS
- Zvažuje sa odstránenie fakturačného kontaktu – využitie?



GDPR z pohľadu registrovania domén (6/7)



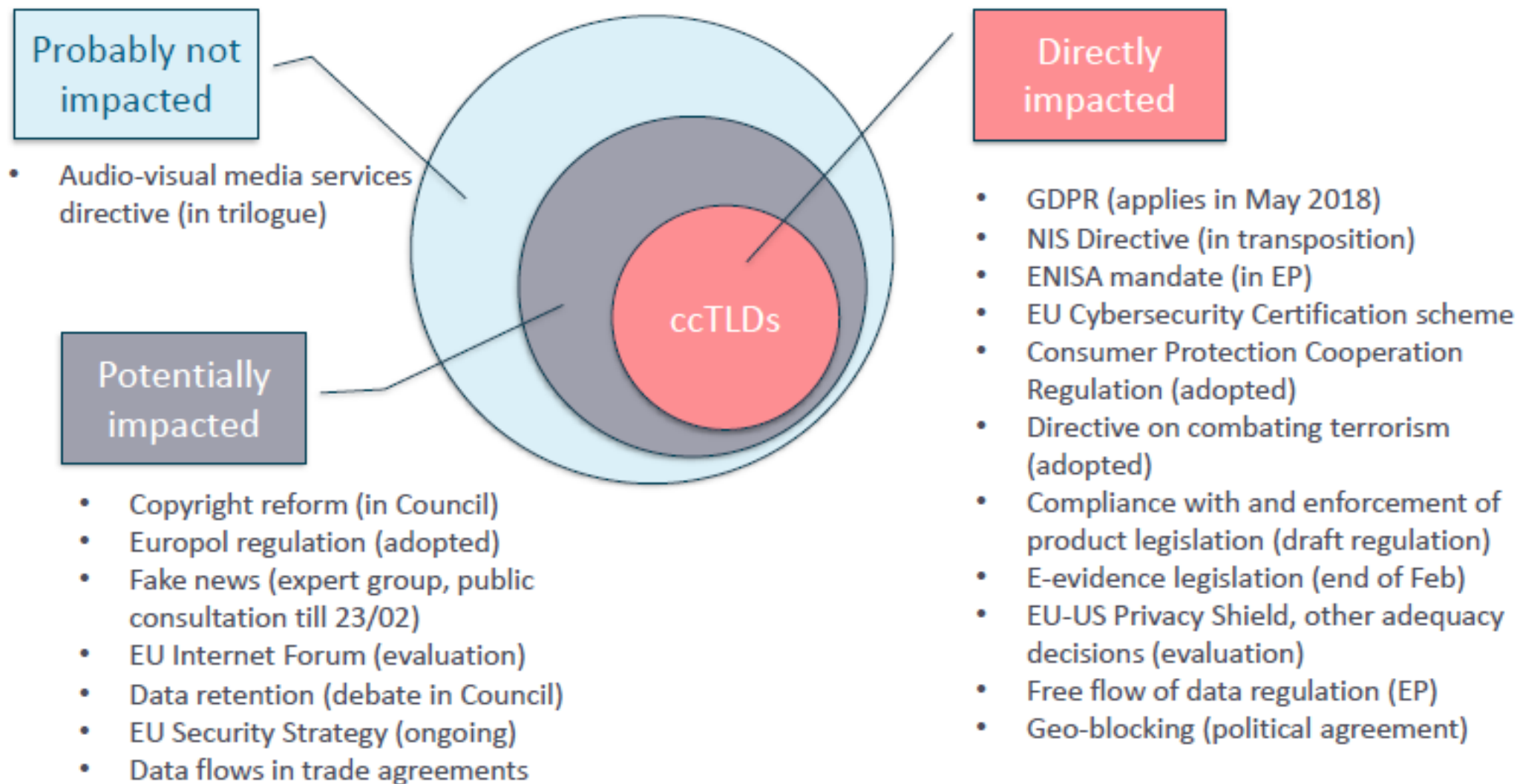
- Činnosti registrátorov nad rámec registrácie domén (vlastné služby – telco, webhosting atď.)
- Bezpečný prístav podľa poskytovateľov služieb informačnej spoločnosti ostáva (napr. webhosting) **(čl. 2, ods. 4)**
- Samostatné poskytovanie povinných informácií používateľovi **(čl. 13 – kontakty, účel...)**
- Nutnosť zodpovednej osoby – „*hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu*“ (~big data) **(čl. 37)**

GDPR z pohľadu registrovania domén (7/7)

- Každý prevádzkovateľ vedie záznamy o spracovateľských činnostiach **(čl. 2, ods. 4) + písm. b)** účely spracúvania = evidencia každého úkonu = logy
 - nepriamo cez ISO 9001 a 27001 aj kto to urobil
- ÚOOÚ: Zamestnanci prevádzkovateľa – oprávnené osoby nie sú príjemcovia



Ďalšia legislatíva (1/3)



Ďalšia legislatíva (2/3)



- Príklady:
- Ochrana spotrebiteľa (**nariadenie 2017/2394**)
 - Právo authority prikázať doménových registrom alebo registrátorom vymazať doménu a zaregistrovať ju na autoritu (**Čl. 9, 4g, iii**)
- Nový návrh – harmonizácia legislatívy ohľadom tovarov (**COM(2017)795**)
 - Právo authority vyžadovať od doménového registra alebo registrátora zablokovanie domény na určené obdobie / jej vymazanie
- NIS (**smernica 2016/1148**) – prevádzkovateľ základných služieb (**príloha II**)
 - 7. Digitálna infraštruktúra – IXP, poskytovatelia služieb DNS, TLD

Ďalšia legislatíva (3/3)



- Digitálne trendy v EÚ (2018):
- Priorita ilegálny obsah – samoregulácia & dobrovoľná aktivita “nie je dostatočná”
- Metodiky sa môžu zmeniť na zákony (oznámenie a odstránenie, IPRED = aut. práva)
- Zvyšuje sa tlak na smernicu ohľadom e-obchodu
- Snahy o opätovnú harmonizáciu ukladania údajov
- Zvyšovanie požiadaviek kybernetickej bezpečnosti
- Väčšie právomoci pre Europol a potenciálne ENISA
- Opätovné ohrozenie EU-US Privacy Shield? (Schrems, WP29, ...)





OTÁZKY ?

Peter Bíro (CEO)