

# OCHRANA OSOBNÍCH ÚDAJŮ (GDPR, ePRIVACY ?)

Jindřich Kalíšek, advokát

Česká advokátní komora 25. 6. 2021



**JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/ECIPM**  
Advokát | Mediátor | Pověřenec pro ochranu OÚ  
Vinohradská 1511 / 230, Praha 10 – Strašnice  
jindrich@kalisek.net (+420) 775 877 046

# PŘEDNÁŠEJÍCÍ

## Jindřich Kalíšek

- / Advokát, zapsaný mediátor  
a pověřenec pro ochranu osobních údajů
- / Člen Odborné sekce ČAK pro právo IT a ochranu  
osobních údajů
- / Spoluautor metodiky k GDPR pro advokáty
- / 12 let praxe v oblasti práva IP/IT, ochrany OÚ  
a kybernetické bezpečnosti



# ORGANIZACE SEMINÁŘE

- / 09:00 – 09:05 *Souboj s Webexem*
- / 09:00 – 10:30 Základní instrumenty GDPR  
Zásady zpracování a ochrany osobních údajů (OÚ)  
Práva subjektů OÚ
- / 10:30 – 10:40 *Přestávka*
- / 10:40 – 11:45 Práva subjektů OÚ  
Specifické povinnosti advokáta coby správce OÚ  
Vybraná témata ke zpracování OÚ
- / 11:45 – 12:00 Q & A (*Pokud Webex dovolí...*)

# AKTUÁLNÍ STAV GDPR

## I

- / Téměř 3 roky po účinnosti GDPR
- / ČR má adaptační legislativu
  - Zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění
  - Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, v platném znění
- / Správci/zpracovatelé OÚ stále „plavou“ v základních principech a požadavcích GPDR
- / Roste sebevědomí DPA a subjektů
  - Přístup ÚOOÚ je značně opatrný
  - Sledování a sankcionování dalších agend

# AKTUÁLNÍ STAV GDPR

## II

### / GDPR v roce tři

- Konec doby hájení ze strany úřadů (ICO v UK, Irsku, CNIL, ÚOOÚ?)
- Konec *documentation-only* přístupu
- Ochrana OÚ v širším kontextu
  - > Ochrana neosobních informací
  - > Informační bezpečnost a kybernetická bezpečnost
- Omezení přeshraničního pohybu OÚ
  - > Brexit (jakoby-rozhodnutí o shodě)
  - > Schrems II (sistace US – EU Privacy Shield)
- První soudní spory
- ~~Kodexy chování~~
- ~~Binding Corporate Rules (BCR)~~

# AKTUÁLNÍ STAV GDPR

## III

### / Přehled sankcí

1. Google – 50 mil. € (CNIL, Francie)  
Mnohočetné, dlouhodobé a systematické porušování zásad zpracování a informační povinnosti
2. H&M – 35 mil. € (Hamburský ÚOOÚ, SRN)  
Neoprávněný monitoring zaměstnanců
3. TIM – 27.8 mil. € (Garante, Itálie)  
Mnohočetné, dlouhodobé a systematické porušování zásad zpracování
4. British Airways – 22 mil. € (ICO, Velká Británie)  
Bezpečnostní incident
5. Marriott – 20.4 mil. € (ICO, Velká Británie)  
Bezpečnostní incident
6. Wind – 17 mil. € (Garante, Itálie)
7. Google – 7 mil. € (SDPA, Švédsko)
8. AOK (Health Insurance) – 1.24 mil. € (ICO, Velká Británie)
9. BKR (National Credit Register) – 830,000 € (ICO, Velká Británie)
10. Iliad Italia – 800,000 € (Garante, Itálie)

# AKTUÁLNÍ STAV GDPR

## IV

### / Správný přístup

- Přinejmenším minimální GDPR compliance v rozsahu 7+2
- Rozumná aplikace požadavků s přihlédnutím k prostředí, potřebám a možnostem organizace a jejímu rizikovému profilu (Výkon advokacie !)
- Integrace do všech procesů a evidencí organizace (i kdyby postupná)
- Zásady ochrany a zabezpečení osobních údajů (čl. 25 + 32 GDPR)
  - > DPIA
  - > Řízené pravidelné zlepšování, řízení změn a pořizování technologií
  - > Vzdělávání a zvyšování risk-awareness

### / Typické rizikové scénáře

- Potěmkinova vesnice × Dělo na vrabce
- Spekulativní ignorace
- Rezignace

# LEGISLATIVNÍ RÁMEC OCHRANY OÚ V EU

- / Nařízení č. 2016/679 – Obecné nařízení o ochraně OÚ (GDPR)
  - Směrnice č. 2016/680 (o ochraně OÚ v trestních věcech)
  - Směrnice č. 2016/681 (PNRD)
  
- / Derogace směrnice č. 95/46/ES o ochraně OÚ  
(*Data Protection Directive*)
  
- / Výkladová praxe WP 29 / EDPB
  - *European Data Protection Board* (EDPB) → náhrada WP 29
  - Vodítko k právu na přenositelnost údajů (WP 242)
  - Vodítko k pověřenci pro ochranu osobních údajů (WP 243)
  - Vodítko k určení vedoucího dozorového úřadu (WP 244)
  - Vodítko k provádění DPIA (WP 248)
  - Stanovisko k zpracování osobních údajů v zaměstnání (WP 249)
  - Vodítko k hlášení porušení zabezpečení ochrany osobních údajů (WP 250)
  - Vodítko k automatizovanému individ. rozhodování a profilování (WP 251)
  - Vodítko k správnímú pokutování (WP 252)
  - Průběžná aktualizace



# LEGISLATIVNÍ RÁMEC OCHRANY OÚ V ČR I

## / Obecné právní předpisy

- Ústava + LZPS
- Z. č. 89/2012 Sb., občanský zákoník
  
- Z. č. 110/2019 Sb., o zpracování osobních údajů (ZZOÚ)
  - > Z. č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím ZZOÚ
  - > Z. č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ)
  
- Z. č. 40/2009 Sb., trestní zákoník
  - > § 180 – Neoprávněné nakládání s osobními údaji
  - > Z. č. 418/2011 Sb., o trestní odpovědnosti PO

## / Úřad na ochranu osobních údajů (ÚOOÚ)

- Výkladová praxe ÚOOÚ

# LEGISLATIVNÍ RÁMEC OCHRANY OÚ V ČR II

- / Zvláštní právní předpisy → 1 300 předpisů hovoří o ochraně OÚ
- Z. č. 262/2006 Sb., zákoník práce + předpisy o zaměstnanosti
  - Z. č. 372/2011 Sb., o zdravotních službách + předpisy o sociální péči
  - Z. č. 111/2009 Sb., o základních registrech + předpisy o ISVS
  - Z. č. 499/2004 Sb., o archivnictví a spisové službě
  - Z. č. 127/2005 Sb., o elektronických komunikacích + novela (ST 1084)
  - Z. č. 480/2004 Sb., o některých službách informační společnosti
  - Z. č. 181/2014 Sb., o kybernetické bezpečnosti
  - Z. č. 284/2009 Sb., o platebním styku + předpisy o finančnictví, pojišťovnictví, bankovníctví a obchodování na finančních trzích
  - Z. č. 280/2009 Sb., daňový řád
  - Z. č. 106/1999 Sb., o svobodném přístupu k informacím
  - Z. č. 256/2013 Sb., katastrální zákon
  - Z. č. 361/2000 Sb., o silničním provozu

# LEGISLATIVNÍ RÁMEC OCHRANY OÚ V ČR

## III

- / Zákon o zpracování osobních údajů (ZZOÚ)
  - Účinný od 24. 4. 2019
  - Provedení GDPR a zčásti implementace směrnice č. 2016/680
  - Obsah
    - > Zpracování OÚ dle GDPR
    - > Zpracování OÚ v trestněprávních věcech
    - > Zpracování OÚ při zajišťování obrany a bezpečnosti
    - > Postavení a pravomoc ÚOOÚ
  - § 64 – Zvláštní právní úprava kontrol ÚOOÚ v advokacii
  - § 63 – Sankce v ČR max. 10 mil. Kč (≈ 390 tisíc €)
    - > Pozor na přeshraniční vyšetřování a ukládání pokut
  
- / Doprovodný změnový zákon
  - Navazuje na návrh ZZOÚ a implementuje směrnice č. 2016/680 a č. 2016/681

# MÍSTNÍ A VĚCNÁ PŮSOBNOST GDPR

## I

- / Čl. 1, 2, 3 a 4 GDPR
- / Cíle Nařízení
  - Ochrana OÚ fyzických osob v EU
  - Volný pohyb OÚ v EU
- / Všechny formy zpracování
  - Zcela/částečně automatizované
  - Manuální, jsou-li anebo mají-li OÚ být součástí evidence
- / Veškeré zpracování OÚ na území EU/EHP, občanů EU a pohyby OÚ v rámci EU/EHP, když:
  - Správce / zpracovatel OÚ sídlí v zemích EU
  - Správce / zpracovatel OÚ nesídlí v zemích EU, ale zpracovává data občanů EU za účelem nabídky zboží, služeb anebo za účelem monitoringu jejich chování na území EU

# MÍSTNÍ A VĚCNÁ PŮSOBNOST GDPR

## II

### / Výluky působnosti GDPR

- Právnícké osoby × ochrana OÚ zaměstnanců
- Zesnulé fyzické osoby a mrtvě narozené děti
- Manuální zpracování neevidovaných OÚ
- Zpracování FO pro výlučně osobní a domácí činnosti
- Zpracování OÚ v oblasti ochrany zákonnosti a bezpečnosti
  - > Výkon činností mimo působnost práva EU
  - > Výkon činností v rámci společné zahraniční a bezpečnostní politiky EU
  - > Prevence, vyšetřování, odhalování a stíhání trestné činnosti
- Anonymní a anonymizované údaje
- (Neidentifikující) údaje pro statistické a výzkumné účely

# VYBRANÉ DEFINICE GDPR

## I

/ Čl. 2, 4 a 9 GDPR

/ Osobní údaje (OÚ) a identifikátory

- „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě,*“
- Subjekt údajů × identifikovatelná osoba
- Identifikátory – „*jméno, identifikační číslo, lokační údaje, síťový identifikátor anebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“

# VYBRANÉ DEFINICE GDPR

## II

### / Čl. 9 GDPR

### / Zvláštní kategorie osobních údajů

- Osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod fyzických osob
  - > Rasový či etnický původ
  - > Genetické údaje a biometrické údaje (za účelem jedinečné identifikace fyzické osoby)
  - > Údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci
  - > Politické názory, náboženské vyznání, filozofické přesvědčení, členství v odborech

# VYBRANÉ DEFINICE GDPR

## III

### / Zpracování

- Jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ
- *Shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*

### / Evidence

- Jakýkoliv strukturovaný soubor OÚ přístupných podle zvláštních kritérií
- Centralizovaný × decentralizovaný
- Rozdělený podle funkčního / zeměpisného hlediska



# VYBRANÉ DEFINICE GDPR

## IV

### / Správce

- Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

### / Zpracovatel

- Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

# VYBRANÉ DEFINICE GDPR

## V

### / Příjemce

- Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty
- Nikoliv orgány veřejné moci v rámci zvláštního šetření v souladu s právem členského státu

### / Porušení zabezpečení osobních údajů (*data breach*)

- Porušení zabezpečení, které vede k náhodnému anebo protiprávnímu zničení, ztrátě, změně anebo neoprávněnému poskytnutí anebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ

# ZÁKAZ ZPRACOVÁNÍ ZVLÁŠTNÍ KATEGORIE OÚ

## / Čl. 9 GDPR

## / Výjimky

- Plnění povinností v oblasti pracovního práva, soc. zabezpečení
  - Ochrana životně důležitých zájmů subjektů údajů nebo jiné FO
  - Některá zpracování neziskovými subjekty
  - OÚ zjevně zveřejněné subjektem údajů
  - Obhajoba právních nároků + zpracování soudy
  - Významný veřejný zájem
  - Účely preventivního nebo pracovního lékařství
  - Veřejný zájem v oblasti veřejného zdraví
  - Archivace ve veřejném zájmu
- 
- Výslovný souhlas subjektu údajů
    - > Ledaže právo stanoví, že subjekt údajů nemůže souhlas platně udělit

# ZÁSADY ZPRACOVÁNÍ OÚ DLE GDPR

## / Zásady zpracování osobních údajů

- Čl. 5 GDPR
- Zásada zákonnosti
- Zásada korektnosti a transparentnosti zpracování
- Zásada účelového omezení shromažďování osobních údajů
- Zásada minimalizace zpracovávání osobních údajů
- Zásada přesnosti osobních údajů
- Zásada omezeného uložení OÚ
- Zásada integrity a důvěrnosti zpracování
- Zásada odpovědnosti

*Advokáti často pro stromy nevidí les...*

# ZÁSADY OCHRANY A ZABEZPEČENÍ OÚ

## I

- / Standardní ochrana OÚ (čl. 25 odst. 2 GDPR)
  - Průmět zásady minimalizace → Přijmout vhodná technická a organizační opatření k minimalizaci zpracovávaných OÚ
  - Povinnost standardně zpracovávat jen OÚ
    - > Nezbytně nutné pro specifikovaný účel
    - > V nezbytně nutném rozsahu
    - > Uchovávat po nezbytně dlouhou dobu
  - OÚ nelze volně zpřístupňovat neomezenému počtu osob
  
- / Záměrná ochrana OÚ (čl. 25 odst. 1 GDPR)
  - Účelem provádět zásady ochrany OÚ a začlenit záruky k ochraně práv subjektů
  - Vhodná technická/organizační opatření k ochraně OÚ → čl. 32 GDPR

# ZÁSADY OCHRANY A ZABEZPEČENÍ OÚ

## II

- / Čl. 32 GDPR – Povinnost zajistit aktivní zabezpečení osobních údajů
- / Příkladný výčet bezpečnostních opatření
  - Povinnost přijmout vnitřní koncepce a vhodná technická a organizační opatření pro zabezpečení zpracování OÚ
  - Zásady záměrné a standardní ochrany osobních údajů
  - Pseudonymizace, šifrování OÚ
  - Neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb
  - Business a data recovery
  - Pravidelné testování, posuzování a hodnocení bezpečnosti opatření

## STATISTIKA NUDA JE...

- / **95 %** incidentů je způsobeno lidskou chybou. (*AT&T*)
- / **314 dní** činil v roce 2019 celý životní cyklus incidentu, z toho 206 dní činila doba k jeho identifikaci. (*IBM*)
- / **4,1 mld. unikátních záznamů** uniklo v data-breaches jen v první polovině roku 2019. (*RiskBased*)
- / **77 % organizací** nemá plán reakce na kybernetické bezpečnostní incidenty. (*AT&T*)
- / **5 % složek souborů** je v organizacích chráněno řádně. 22 % složek je k dispozici každému. (*Varonis*)
- / **61 % společností** má více než 500 účtů, jejichž hesla nevyprší. (*Varonis*)
- / **300 mld.** činí odhadovaný počet hesel na celém světě v roce 2020. (*Cybersecurity Media*)
- / **62 % podniků** zažilo v roce 2018 útoky na bázi phishingu a sociálního inženýrství. (*Cybint Solutions*)
- / **300% nárůst hlášených počítačových zločinů** v souvislosti s pandemií COVID-19 (*FBI*)

# KONKRÉTNÍ OPATŘENÍ K ZAJIŠTĚNÍ BEZPEČNOSTI OÚ

## / Právní × Organizační × Technická

- Poučení o právech a povinnostech zaměstnanců
- Postup při ukončení pracovního poměru
  - > Předání přidělených aktiv, zrušení přístupových práv, poučení o následcích porušení zákonné nebo smluvní povinnosti mlčenlivosti
- Vedení seznamu aktiv a jeho aktualizace, řízení změn
- Kontrola vstupu do objektu a chráněných prostor, správa klíčů
- Přidělování přístupových práv a úrovní přístupu (rolí) oprávněných osob a správa hesel
- Vzájemné zastupování oprávněných osob
- Režim údržby a úklidu chráněných prostor
- Pravidla manipulace s fyzickými nosiči OÚ mimo chráněné prostory
- Pravidla užívání IT prostředků (např. notebooky) mimo chráněné prostory
- Pravidla užívání přenosných datových nosičů mimo chráněné prostory
- Určení postupů likvidace osobních údajů s vymezením související odpovědnosti jednotlivých oprávněných osob



# PRÁVNÍ TITULY ZPRACOVÁNÍ OÚ DLE GDPR

## / Zákonné tituly pro zpracování osobních údajů

- Čl. 6 GDPR
- Splnění smlouvy
- Splnění právní povinnosti
- Ochrana životně důležitých zájmů subjektu údajů anebo jiné fyzické osoby
- Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněné zájmy příslušného správce anebo třetí strany

- 
- Souhlas subjektu údajů

# NAPLŇOVÁNÍ PRÁV SUBJEKTŮ

## / Čl. 12 – 23 GDPR

- Právo na informace o zpracování OÚ

---

- Právo na přístup subjektu k OÚ
  - > Právo získat od správce OÚ potvrzení o zpracování OÚ
  - > Právo získat kopii zpracovávaných OÚ
- Právo na opravu
- Právo na výmaz („*právo být zapomenut*“)
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů
- Právo nebýt předmětem automatizovaného rozhodnutí

/ Ochrana soukromí je obvykle v přímé kolizi s jinými právy →  
nemůže být absolutní

# INFORMAČNÍ POVINNOST VŮČI SUBJEKTŮM I

- / Naplňování informační povinnosti vůči subjektům (čl. 12 – 14 GDPR)
  - Zásada transparentního zpracování (čl. 5 odst. 1 písm. a) GDPR)
  
- / Informační povinnost
  - Před / na začátku zpracování
  - V průběhu zpracování → komunikace směrem k subjektům
  - V mimořádných situacích (zejm. *data breach*)
  
- / Informační povinnost podle adresátů:
  - Vůči subjektům
  - Vůči dozorovému úřadu (ohlašovací povinnosti)
  - Vůči příjemcům OÚ
  - Lze mít jednu generální × více zvláštních informací
  
- / Informování nutno v případě kontroly prokázat

# INFORMAČNÍ POVINNOST VŮČI SUBJEKTŮM II

- / Čl. 12 GDPR
  - Pokyny WP29 k transparentnosti (WP260)
  
- / Veškeré informace a sdělení dle GDPR musí být:
  - Poskytnuty stručným, transparentním, srozumitelným a snadno přístupným způsobem → možno doplnit standardizovanými ikonami
  - Za použití jasných a jednoduchých jazykových prostředků
  - Písemně nebo jinými prostředky (včetně elektronické formy) → i ústně
  - Bezplatně
  
- / Výjimky z informační povinnosti
  - Čl. 13 GDPR → Subjekt již uvedené informace má (a do té míry, v níž je má)
  - Čl. 14 GDPR → Subjekt uvedené informace má, poskytnutí není možné / vyžadovalo by nepřiměřené úsilí, získávání či zpřístupnění je stanoveno právem EU nebo členského státu, služební tajemství / mlčenlivost
  - § 10 návrhu zákona o zpracování OÚ

# PŘESTÁVKA



# DALŠÍ PRÁVA SUBJEKTŮ OÚ

## I

- / Čl. 15 GDPR: Právo SÚ na přístup k OÚ → právo získat od správce na žádost
  - Potvrzení, zda jsou OÚ subjektu zpracovávány
  - Přístup k těmto OÚ (kopie zpracovávaných osobních údajů)
  - Přístup k určitým informacím
  
- / Poskytované informace
  - Účely zpracování
  - Kategorie dotčených osobních údajů
  - Příjemci nebo kategorie příjemců
  - Doba zpracování
  - Existence práv subjektu (oprava, výmaz, omezení zpracování, námitka, podat stížnost u dozorového orgánu)
  - Zdroj, od kterého byly údaje získány
  - Zda dochází k automatizovanému rozhodování
  - Při předání OÚ do třetí země – vhodné záruky předání
  
- / Požadavky na sdělení shodné jako u práva na informace

# DALŠÍ PRÁVA SUBJEKTŮ OÚ

## II

- / Formát poskytovaných informací
  - / Lhůta k vyřízení
    - Bez zbytečného odkladu → do 1 měsíce (možno výjimečně prodloužit)
    - Nevyhovění žádosti: bez zbytečného odkladu → do 1 měsíce
  - / Náhrada nákladů
    - Informace se poskytují bezplatně, ledaže jsou žádosti zjevně nedůvodné nebo nepřiměřené (přiměřený poplatek / odmítnutí žádosti)
  - / Právem získat kopii nesmějí být nepříznivě dotčena práva jiných osob
- 
- / Zákon o zpracování osobních údajů
    - § 28 odst. 2 – omezení práva na přístup – je-li to nezbytné a přiměřené pro ochranu práv jiné osoby
    - § 28 odst. 4 a § 29 odst. 6 – dokumentace o uplatnění práv se uchovává po dobu 3 let

# DALŠÍ PRÁVA SUBJEKTŮ OÚ

## III

- / Čl. 17 GDPR – Právo subjektu na vyžádaný výmaz jeho OÚ
- / Správce má povinnost bez zbytečného odkladu vymazat OÚ subjektu a nesmí je dále zpracovávat
  - Již nejsou potřebné pro původní účely
  - OÚ shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti
  - Subjekt údajů odvolal svůj souhlas
  - Zpracování OÚ je anebo se v průběhu času stane protiprávním
  - Právo subjektu žádat o výmaz osobních údajů, které se jej týkají
- / Správce může žádost odmítnout, pokud je zpracování nezbytné pro
  - Výkon práva na svobodu projevu a informace
  - Splnění právní povinnosti správce podle práva Unie nebo čl. státu
  - Veřejný zájem v oblasti veřejného zdraví
  - Archivaci ve veřejném zájmu, výzkum, statistické účely
  - Určení, výkon nebo obhajobu právních nároků



# DALŠÍ PRÁVA SUBJEKTŮ OÚ

## IV

- / Čl. 20 GDPR – Právo na přenos OÚ (*Data portability*)
  - Vodítko WP 29 k právu na přenositelnost (WP 242 rev. 01)
  - Právo subjektu na žádost získat „své“ osobní údaje
  - Právo subjektu předat tyto údaje jinému správci (ideálně přímo od správce k správci)
  
- / Podmínky práva na přenositelnost
  - Zpracování se provádí automatizovaně (forma zpracování)
  - Zpracování na základě předchozího souhlasu nebo k naplnění smlouvy, jejíž stranou je SÚ (důvod zpracování), získané sledováním jeho chování × ne data získaná technikou anebo jinou analýzou
  - Osobní údaje se týkají SÚ a byly poskytnuty SÚ (rozsah přenášených osobních údajů, kategorie dat v závislosti na jejich původu)
  - Právo na přenositelnost se neuplatní na zpracování osobních údajů ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen
  - Výměnný formát → strukturovaný, strojově čitelný, běžně používaný

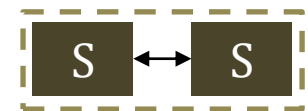
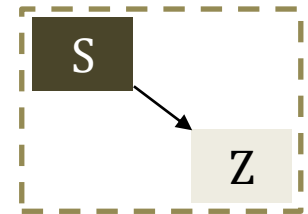
# DALŠÍ PRÁVA SUBJEKTŮ OÚ

## V

- / Čl. 21 GDPR: Právo subjektu OÚ vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů
  - Správce má povinnost prokázat, že jeho zájmy převažují nad oprávněnými zájmy namítatele
  - Informační povinnost správce
  
- / Čl. 22 GDPR: Právo subjektu nebýt předmětem automatizovaného individuálního rozhodnutí (včetně profilování)
  - Pakliže se jej významně dotýká
  - Pakliže pro něj má právní účinky

# SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ I

- / Smlouva o zpracování osobních údajů
  - Čl. 28 GDPR → minimální obsah v odst. 3
  - Smlouva mezi správcem a zpracovatelem
  
- / Smlouva o společné správě osobních údajů
  - Čl. 26 GDPR
  - Smlouva o rozdělení kompetencí a odpovědností mezi správci, kteří vykonávají společnou správu osobních údajů
  
- / Smlouva o nakládání s osobními údaji / o předávání osobních údajů
  - Není v GDPR zakotvena
  - Mezi samostatnými správci, kteří však nevykonávají společnou správu
  - Vymezuje odpovědnost při nakládání s osobními údaji
  
- / Postavení správce / zpracovatel
  - Správce sám nebo společně s jinými určuje účely a prostředky zpracování OÚ a uděluje pokyny zpracovateli
  - Zpracovatel zpracovává OÚ pro správce → na základě pokynů správce



# SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ II

- / Smlouva o zpracování osobních údajů (čl. 28 GDPR)
  - Správce využije pouze ty zpracovatele, kteří poskytují dostatečné záruky naplnění požadavků GDPR a zavedení vhodných TOMs
  - Zpracovatel nesmí zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce
  - Zpracovatel zpracovává OÚ na základě písemné smlouvy nebo jiného právního aktu podle práva EU nebo členského státu
- / Minimální obsah → odst. 3
  - Předmět a doba trvání zpracování
  - Povaha a účel zpracování
  - Typ OÚ a kategorie subjektů údajů
  - Povinnosti a práva správce

# SMLOUVY O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ III

## / Minimální obsah → odst. 3

- Povinnosti zpracovatele
  - > Zpracovávat OÚ pouze na základě doložených pokynů správce
  - > Zajistit, aby se osoby zpracovávající OÚ se zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti
  - > Přijmout všechna (?) TOMs podle čl. 32 GDPR
  - > Zohlednit povahu zpracování
  - > Být správci nápomocen pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů, při zajišťování souladu s povinnostmi v oblasti zabezpečení OÚ, hlášení bezpečnostních incidentů a provádění DPIA
  - > Podle rozhodnutí správce po ukončení zpracování všechny OÚ vymazat nebo je vrátit správci a vymazat existující kopie
  - > Poskytnout správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v čl. 28
  - > Umožnit audity a inspekce prováděné správcem nebo jiným auditorem, kterého správce pověřil

# HLÁŠENÍ BEZPEČNOSTNÍCH INCIDENTŮ

- / Povinnost zajistit odpovídající zabezpečení OÚ (čl. 32 GDPR)
- / Povinnost ohlašovat bezpečnostní incidenty (*data breaches*)
  - Jakékoliv porušení zabezpečení
    - > Výjimka: Nepravděpodobnost rizika pro práva a svobody FO
  - Bez zbytečného odkladu, nejpozději do 72 hodin dozorovému orgánu
  - Bez zbytečného odkladu v případě závažného úniku i subjektům OÚ
  - Dokumentace **všech** incidentů
- / Obsah ohlášení
  - Popis povahy incidentu, včetně kategorie a počtu dotčených subjektů a OÚ
  - Jméno a kontaktní údaje pověřence (jiného kontaktního místa)
  - Popis pravděpodobných důsledků
  - Popis opatření (přijatých/navržených)

# POSOUZENÍ VLIVU NA ZPRACOVÁNÍ OÚ

- / Čl. 35 – 36 GDPR + Vodítko WP 29 (WP 248)
- / Povinnost provést posouzení vlivu na ochranu OÚ (*DPIA*)
  - Každé stávající nebo připravované zpracování OÚ
  - Posouzení vlivu konkrétních operací při zpracování OÚ, které představují nebo mohou představovat vysoké riziko pro práva a svobody FO
    - > Systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování (včetně profilování)
    - > Rozsáhlé zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se trestních věcí
    - > Rozsáhlé systematické monitorování veřejně přístupných prostorů
- / Povinnost předchozí konzultace s dozorovým úřadem
  - Pokud je identifikováno vysoké riziko, které nelze eliminovat

# PŘESHraniční ZPRACOVÁNÍ OÚ MIMO EU I

- / Předávání OÚ v rámci EU → svoboda pohybu osobních údajů ×
  - Předávání OÚ do třetích zemí nebo mezinárodním organizacím
  
- / Obecná zásada bezpečnosti zpracování
  - K předání osobních údajů může dojít pouze tehdy, splní-li správce/zpracovatel podmínky nařízení
  - Úprava předání OÚ – cílem zajistit, aby úroveň ochrany FO zaručená GDPR nebyla znehodnocena
  
- / Varianty předávání osobních údajů
  - Předávání založené na rozhodnutí o odpovídající ochraně
  - Předávání založené na vhodných zárukách
  - Předávání založené na výjimkách



# PŘESHraniční ZPRACOVÁNÍ OÚ MIMO EU II

- / Rozsudek Soudního dvora Evropské unie ve věci C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited a Maximilian Schrems* ze dne 16. 7. 2020 (**Schrems II**)
  
- / Dopady
  - Zneplatnění prováděcího rozhodnutí EK ze dne 12. 7. 2016 podle DPD o odpovídající úrovni ochrany poskytované štítem EU–USA (*EU-US Privacy Shield*)
    - > Při exportu OÚ mimo EU je nutné zajistit vhodné záruky podle čl. 46 GDPR
    - > Americká legislativa (FISA 702) neposkytuje dostatečné záruky (pravomoci tajných služeb)
  - Rozhodnutí EK 2010/87 ze dne 5. 2 2010 o standardních smluvních doložkách (SCC) platné
    - > Je na odpovědnosti vývozce a dovozce osobních údajů, aby poskytli dodatečné záruky
    - > Součinnost národních DPA s EDPB
  
- / EDPN – *Recommendations on supplementary measures following Schrems II*

# POVĚŘENEC PRO OCHRANU OÚ (DPO)

- / Čl. 37 a násl. GDPR + Vodítko WP 29 o pověřencích (WP 243 rev. 01)
- / Kdo musí jmenovat pověřence?
  - Každý orgán veřejné moci nebo veřejný subjekt
  - Subjekty provádějící v rámci svých hlavních činností:
    - > Rozsáhlé pravidelné a systematické monitorování subjektů OÚ
    - > Rozsáhlé zpracování OÚ zvláštní kategorie a údajů týkajících se rozsudků ve věcech trestních
  - Ten, po němž to bude vyžadovat právo EU anebo právo členského státu EU
- / Klíčové úkoly DPO
  - Monitorování zpracování OÚ s cílem zajistit soulad s GDPR a zajišťování provádění práv subjektů údajů
  - Posuzování vlivu na zpracování OÚ (DPIA, konzultace s dozorovým orgánem)
  - Ohlašování a řešení bezpečnostních incidentů
  - Konzultace a odborná vyjádření, vzdělávání a školení zaměstnanců a externích dodavatelů
- / Jmenování DPO v advokátní praxi:
  - Jednotlivý advokát nebo jen velká advokátní kancelář?

# OCHRANA OÚ V ADVOKACII

## I

### / Oborové právní předpisy

- Z. č. 85/1996 Sb., o advokacii
- V. č. 176/2010 Sb., o identifikačních průkazech advokátů
- V. č. 275/2006 Sb., zjišťování poměrů žadatele o určení advokáta ČAKem
  
- Usnesení ČAK
  - > č. 1/1997 Věstníku - etický kodex
  - > č. 9/1999 Věstníku - podrobnosti a dokumentaci advokáta
  - > č. 7/2004 Věstníku - o provádění úschov peněz
  - > č. 4/2006 Věstníku - o povinnostech při ověřování podpisů
  - > č. 2/2008 Věstníku - o povinnostech ve vztahu k AML
  
- Z. č. 358/1992 Sb., notářský řád
- Z. č. 202/2012 Sb., o mediaci
- Z. č. 312/2006 Sb., o insolvenčních správcích
- Z. č. 120/2001 Sb., exekuční řád
- Z. č. 26/2000 Sb., o veřejných dražbách
- Z. č. 36/1967 Sb., o znalcích a tlumočnících

# OCHRANA OÚ V ADVOKACII

## II

- / Obecné (procesní) právní předpisy – postavení a postupy
  - Občanský soudní řád, trestní řád, správní řád, daňový řád
  - Insolvenční řád, exekuční řád
  
- / Výkladová praxe ÚOOÚ
  - Stanovisko č. 7/2006 - Dozorové pravomoci Úřadu pro ochranu osobních údajů v souvislosti s výkonem advokacie
  - Stanovisko č. 4/2006 - Zveřejňování osobních údajů v dražební vyhlášce
  
- / Oborové kodexy chování (čl. 40 GDPR)
  - Bude mít advokacie svůj kodex nebo jinou formu závazných pravidel?
    - > Kodex Slovenské advokátské komory (SAK)
    - > 12 doporučení Irské advokátní komory (LSI)
    - > Kodex aténské komory (ABA)
    - > Doporučení CCBE

# SPECIFIKA V ADVOKACII A PRÁVNÍ PRAXI I

- / Mlčenlivost × Výkon kontroly dozorového úřadu
  - § 21 zákona o advokacii ← Nález II. ÚS 889/10
  - Judikatura NSS
    - > Činnost advokátů a dozor ÚOOÚ (2 As 21/2011-166, 1As 13/2011)
    - > Ochrana advokátní korespondence (5 Afs 95/2007)
  
- / Prohlídka advokátní kanceláře
  - §85b trestního řádu – domovní prohlídka (stanovisko trestního kolegia NS ČR Tpjn 306/2014)
  - §255 daňového řádu – pouze za přítomnosti a se souhlasem zástupce ČAK
  
- / Vedení clientského spisu advokátem
  - Usnesení představenstva ČAK č. 9/1999 Věstníku
  - § 25 ZA - o poskytování právních služeb je advokát povinen vést přiměřenou dokumentaci
  - Skartační lhůta 5 let (pokud právní nebo zvláštní stavovský předpis nestanoví jinak – např. AML)
  - Předložení dokumentace členu kontrolní rady ČAK

# SPECIFIKA V ADVOKACII A PRÁVNÍ PRAXI II

- / Vedení evidence provedených konverzí a osvědčení pravosti podpisu
  - Z. č. 300/2008 Sb. – vedení evidence, uchování po dobu 10 let
  - Zasílání přehledu provedených konverzí ČAK (měsíčně, elektronicky)
  - O všech učiněných prohlášeních o pravosti podpisu formou knihy o prohlášeních o pravosti podpisu
  - Okruh subjektů, kterým může být kniha zapůjčena (ČAK, Ministerstvo spravedlnosti, soudy, OČTR, ustanovený znalec)
  
- / Povinnosti ze z. č. 253/2008 Sb. – AML
  - Povinné osoby (§ 2) – notář při úkonech v rámci notářské úschovy, advokát/notář při úschově peněz, cenných papírů nebo jiného majetku svého klienta, soudní exekutor při provádění další činnosti exekutora podle exekučního řádu a při úschově peněz, cenných papírů nebo jiného majetku
  - Jestliže klientem požadované služby mají spočívat nebo spočívají v jednání jménem klienta nebo na jeho účet při
    - > obstarávání koupě nebo prodeje nemovitosti nebo obchodního závodu anebo jeho části,
    - > správě peněz, cenných papírů, obchodních podílů nebo jiného majetku svého klienta,
    - > zakládání, řízení nebo provozování obchodní společnosti aj.
    - > inkasu, platbách, převodech, vkladech nebo výběrech prováděných při bezhotovostním i hotovostním platebním styku

# SPECIFIKA V ADVOKACII A PRÁVNÍ PRAXI III

## / Povinnosti ze z. č. 253/2008 Sb. – AML

- Soubor zvláštních povinností identifikace povinnou osobou
  - > Identifikace: Vznik obchodního vztahu, obchod nad 1000 € a podezřelý obchod
  - > Kontrola: Obchod mimo obchodní vztah s hodnotou nad 15 000 €, politicky exponovaná osoba, osoba z rizikové země × průběžně při obchodním vztahu
- Povinnost informace uchovávat
- Povinnost hlásit podezřelé obchody
- Problematická praxe pomocí sběru a uchování kopie OP

# MINIMÁLNÍ ROZSAH GDPR COMPLIANCE

## 7 + 2 povinností správce osobních údajů

- / Dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení osobních údajů (čl. 5, 6, 9, 25 a 32 GDPR)
- / Vedení záznamů o činnostech zpracování (čl. 30 GDPR)
- / Zavedení systému procesů reakcí na práva subjektů (čl. 15 – 22 GDPR)
- / Naplňování informační povinnosti vůči subjektům (čl. 12 – 14 GDPR)
- / Identifikace, dokumentace a hlášení bezpečnostních incidentů na poli osobních údajů (čl. 35 GDPR)
- / Revize smluv se zpracovateli osobních údajů (čl. 26 a 28 GDPR)
- / Systém sběru, evidence a zpracování souhlasů se zpracováním OÚ (čl. 7 – 8 GDPR)
  
- / Zavedení DPO do organizace a vybavení odpovídajícími kompetencemi
- / Provedení úvodní DPIA v oblastech, kde bude identifikováno vysoké riziko zpracování osobních údajů



# Q & A

# Děkuji za Vaši pozornost

Jindřich Kalíšek, advokát

[jindrich@kalisek.net](mailto:jindrich@kalisek.net)

(+ 420) 775 877 046



**JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/ECIPM**

Advokát | Mediátor | Pověřenec pro ochranu OÚ

Vinohradská 1511 / 230, Praha 10 – Strašnice

[jindrich@kalisek.net](mailto:jindrich@kalisek.net) (+420) 775 877 046