CYBERLAWYER

OCHRANA OSOBNÍCH ÚDAJŮ (GDPR A ČESKÁ PRÁVNÍ ÚPRAVA)

Jindřich Kalíšek, advokát

Česká advokátní komora | Online | 5. 11. 2025

JINDŘICH KALÍŠEK

JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/E CIPM FIP

- Advokát a zakladatel CYBERLAWYER
- Hlavní architekt regfor
- Vysokoškolský učitel na Právnické fakultě UK
- Člen Spolku pro ochranu osobních údajů
  - Předseda Komise pro kyberbezpečnost
- 5+ let praxe pověřence pro ochranu osobních údajů
  - 50+ compliance projektů v oblasti ochrany osobních údajů (OÚ), informační a kybernetické bezpečnosti (IKB)
  - Pověřenec roku 2019 v soukromoprávní oblasti

ORGANIZACE SEMINÁŘE

- 09:00 – 10:30 **Blok 1 – Legislativní rámec a judikatura v oblasti OÚ**
  Desatero klíčových povinností dle GDPR
  Základní pojmy, zásady a instrumenty GDPR
  Přehled klíčové judikatury, doporučení a rozhodnutí v oblasti zpracování a ochrany OÚ
- 10:30 – 10:45 Přestávka + Podpis výkazů
- 10:45 – 11:50 **Blok 2 – Vybrané povinnosti regulovaných subjektů**
  Práva subjektů OÚ
  Specifické povinnosti advokáta coby správce OÚ
  Vybraná témata zpracování OÚ

1

LEGISLATIVNÍ RÁMEC A JUDIKATURA V OBLASTI OÚ

- Desatero klíčových povinností dle GDPR
- Základní pojmy, zásady a instrumenty GDPR
- Přehled klíčové judikatury, doporučení a rozhodnutí v oblasti OÚ

AKTUÁLNÍ TRENDY V OBLASTI REGULACE OÚ

- Regulace zpracování, ochrany a zabezpečení OÚ tvoří stále robustnější jádro digitální compliance

- Regulace OÚ se „reinstaluje“ spolu s novými předpisy *Digitální dekády*
  - > Digitální služby (DA, DMA, DGA, DSA ad.)
  - > Kybernetická bezpečnost (NIS2, CER, CRA, DORA, AIA)
  - > Umělá inteligence (AIA)

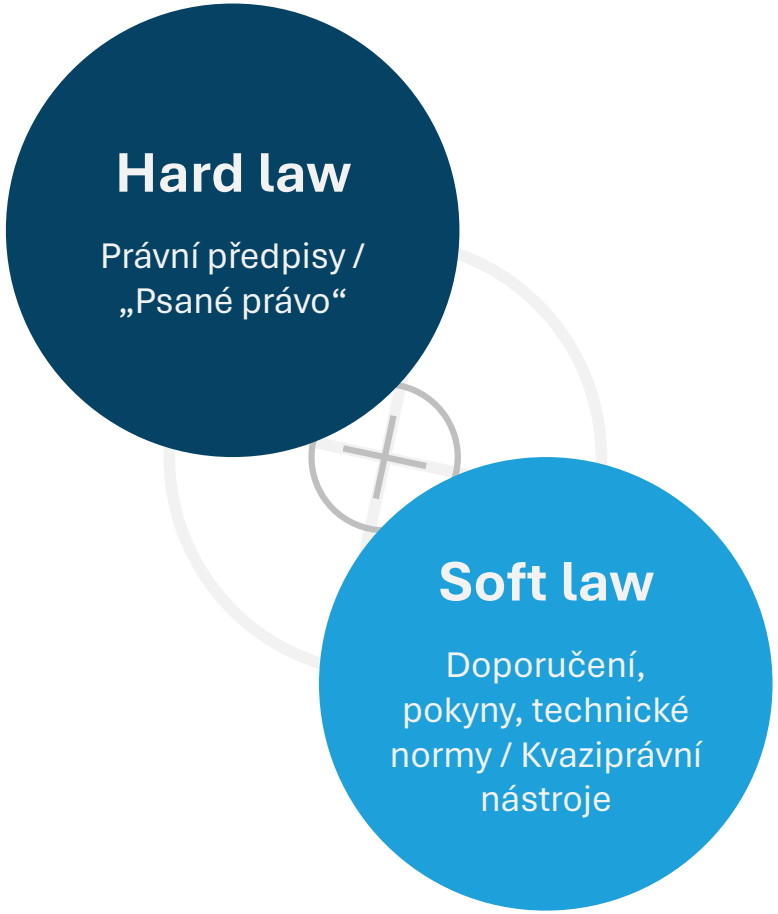
- Sebevědomá aktivita evropských DPA a NGO **× frivolní přístup subjektů údajů**
  - > Postihování „vedlejších“ agend (nevyžádaná obchodní sdělení, informační povinnost, cookies, vedení záznamů o činnostech zpracování)
  - > Stále objemnější rozhodovací praxe SDEU, národních DPA, soudů
  - > Digitální aktivismus (NOYB – Schrems I / II / III)

ZMĚNA PARADIGMAT REGULACE

- Široká aplikace zásady přiměřenosti *(proporcionality)*
- Široká aplikace principu odpovědnosti *(accountability)*
  - > Posun od behaviorální (metodické) k performativní regulaci
  - > Povinný dokládá obecnou i sektorovou compliance i vhodnost, realizaci a efektivitu opatření
- Požadavek vysoké transparentnosti *(transparency)*
- Nutná promyšlená kombinace opatření
  - > Technická × Organizační **(× Provozní × Administrativní × Právní)**

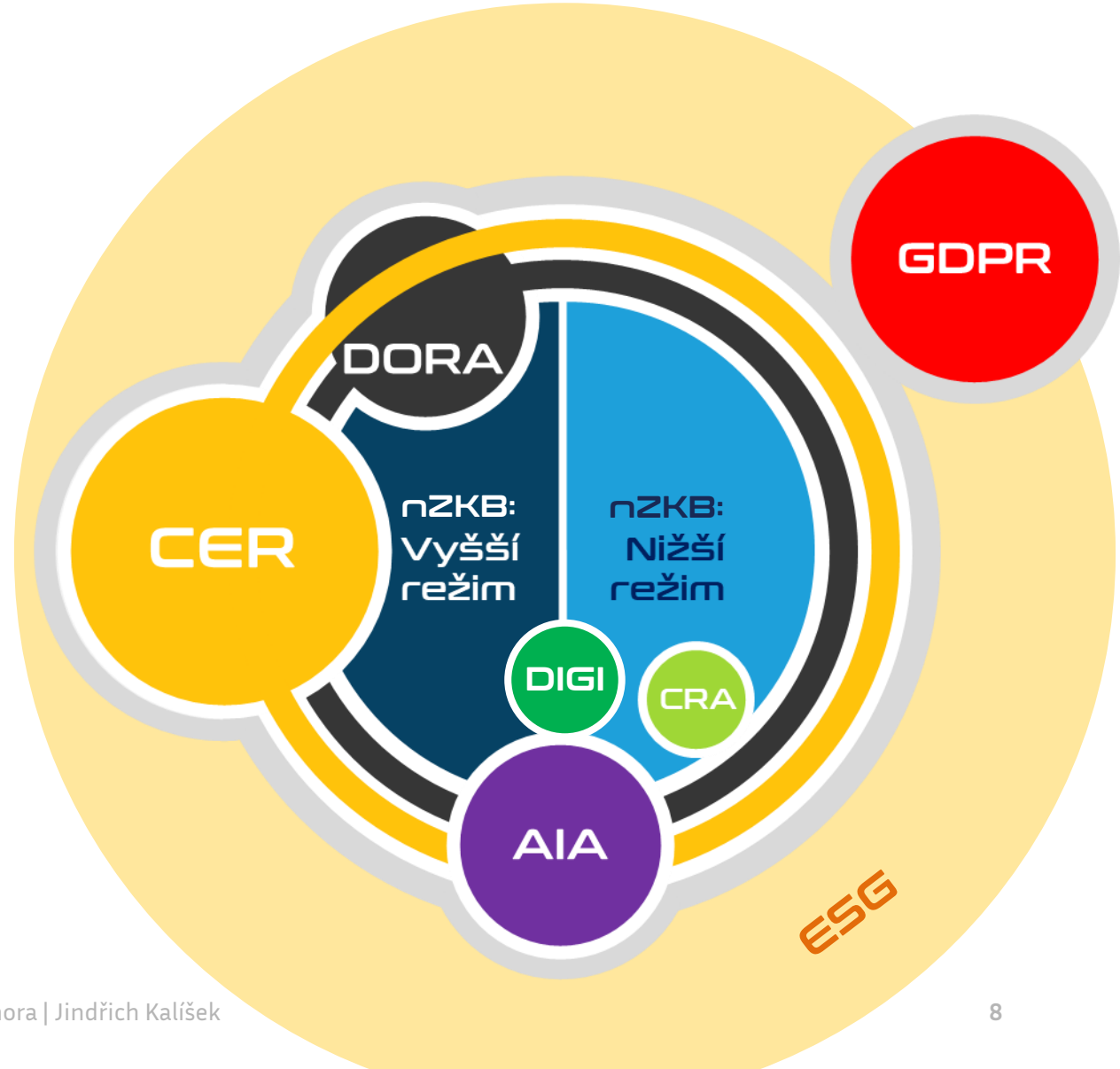
SOFT WITH LAW? TRY SOFT LAW!

- Soft law
  - > Není primárně závazné, přímo vynutitelné výkonnou a soudní mocí → ovlivňuje však chování adresátů
    - > Zásada legitimního očekávání (SDEU C-189/02 P, Dansk Rørindustri A/S)
  - > Vydávané orgány veřejné správy i soukromoprávními subjekty → spontánní (samo)regulace
- Příklady
  - > Doporučení a deklarace mezinárodních organizací
  - > Doporučení a pokyny orgánů EU a vnitrostátních orgánů
  - > Výkladová stanoviska orgánů, profesních organizací apod.
  - > Samoregulační kodexy
  - > Technické normy vč. ISO norem



EXPOZIČNÍ ANALÝZA

- **nZKB (NIS2):** Plníme vymezená kritéria?
  - > Plníme velikostní kritéria / věcná kritéria (§ 4 a 5)?
  - > Jaký režim povinností na nás dopadá (§ 8)?
  - > Kalkulačka NÚKIB
- **DORA:** Jsme finanční subjekt či dodavatel IKT podle definice?
- **nZKI (CER):** Jsme subjekt kritické infrastruktury?
- **CRA / AIA:** Uvádíme na trh EU výrobek anebo službu, která odpovídá definici?
- **DIGI (2024/2690):** Jsme poskytovatel digitální služby podle definice?

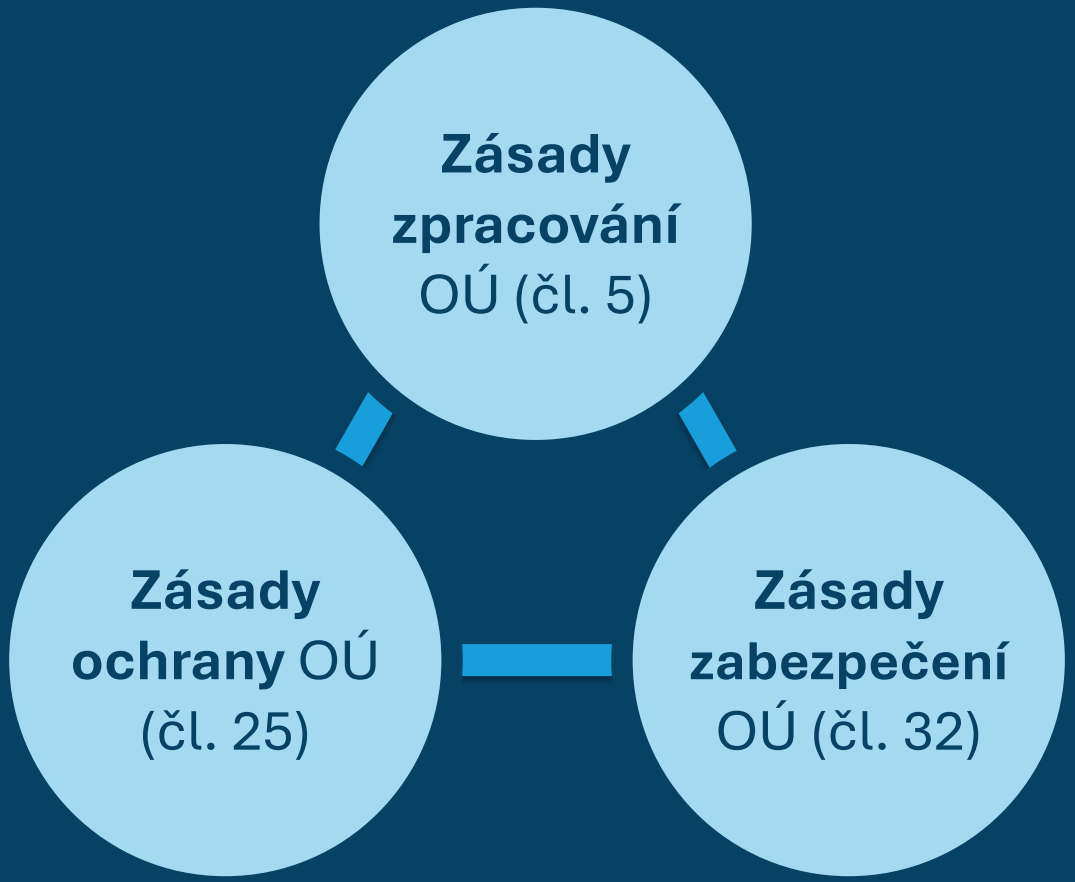


DESATERO GDPR COMPLIANCE (7+3)

- Aktuální dokumentace naplňování zásad zpracování, ochrany a zabezpečení OÚ dle čl. 5, 6, 25 a 32 GDPR
- Aktuální záznamy o zpracování OÚ dle čl. 30 GDPR
- Naplňování informační povinnosti vůči subjektům údajů dle čl. 12 – 14 GDPR
- Proces naplňování práv subjektů údajů dle čl. 15 – 24 GDPR a vedení jejich evidence
- Proces identifikace, vyhodnocení a hlášení bezpečnostních incidentů a vedení jejich evidence
- Revize a renegociace smluv → smlouvy o zpracování OÚ dle čl. 28 GDPR
- Systém evidence souhlasů subjektů se zpracováním OÚ

- Ustavení a zajištění funkce DPO
- Provedení posouzení vlivů na zpracování OÚ (DPIA)
- Pravidelné zlepšování, zajišťování awareness a testování prostředí

ZÁKLADNÍ ZÁSADY GDPR



Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů.

- Základní právní rámec GDPR
  - > Zásady zpracování – Jak data zpracovávat? Co s nimi lze dělat?
  - > Zásady ochrany – Jak data účelně chránit?
  - > Zásady zabezpečení – Jak data zabezpečit? ← narušení CIA + autenticity?
  - > Spojení pohledu soukromí (privacy) a bezpečnosti (security)

ZÁSADY ZPRACOVÁNÍ OÚ

- 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 rádi pro stromy nevidí les…

ZÁSADY OCHRANY OÚ

- 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

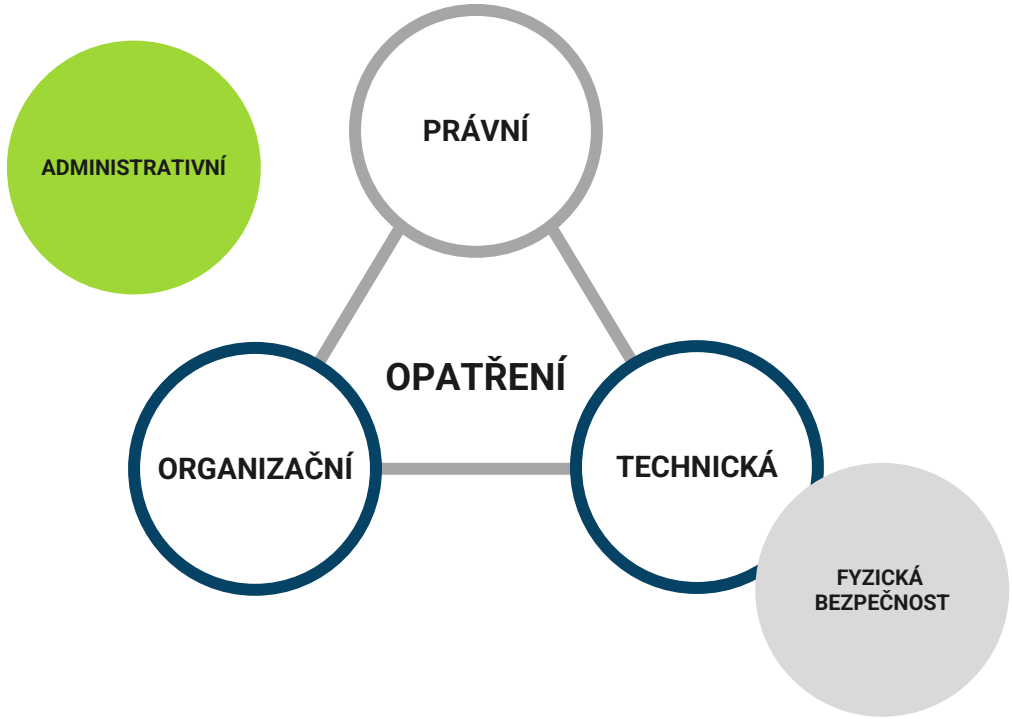
ZÁSADY ZABEZPEČENÍ OÚ

- 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 continuity a data recovery
  - Pravidelné testování, posuzování a hodnocení bezpečnosti opatření

ZAVÁDĚNÍ BEZPEČNOSTNÍCH OPATŘENÍ

- V GDPR se zásady ochrany OÚ promítají
  - Přístup založený na riziku (*risk-based approach*)
  - Zásady zpracování OÚ (čl. 5 odst. 1 GDPR)
  - Záměrná a standardní ochrana OÚ (čl. 25 odst. 1 a 2 GDPR)
  - Požadavky na technická a organizační opatření (čl. 32 GDPR)
- Organizační a technická opatření
  - Ochrana před nějakou hrozbou / snížení zranitelnosti / omezení vlivu nechtěné události / umožnění zotavení organizace
  - Kombinace přístupů, praktik, procedur a mechanismů



BEZPEČNOSTNÍ OPATŘENÍ PODLE NZKB

Organizační opatření

a) systém řízení bezpečnosti informací
b) povinnosti vrcholného vedení
c) bezpečnostní role
d) řízení bezpečnostní politiky a bezpečnostní dokumentace
e) řízení aktiv
f) řízení rizik
g) řízení dodavatelů
h) bezpečnost lidských zdrojů
i) řízení změn
j) akvizice, vývoj a údržba
k) řízení přístupu
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
m) řízení kontinuity činností
n) audit kybernetické bezpečnosti

Technická opatření

a) fyzická bezpečnost
b) bezpečnost komunikačních sítí
c) správa a ověřování identit
d) řízení přístupových oprávnění
e) detekce kybernetických bezpečnostních událostí
f) zaznamenávání bezpečnostních a relevantních provozních událostí
g) vyhodnocování kybernetických bezpečnostních událostí
h) aplikační bezpečnost
i) kryptografické algoritmy
j) zajišťování dostupnosti regulované služby
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Organizační a technická opatření

a) systém zajišťování minimální kybernetické bezpečnosti
b) požadavky na vrcholné vedení
c) řízení aktiv
d) řízení rizik
e) bezpečnost lidských zdrojů
f) řízení kontinuity činností
g) řízení přístupu
h) řízení identit a jejich oprávnění
i) detekce a zaznamenávání kybernetických bezpečnostních událostí
j) řešení kybernetických bezpečnostních incidentů
k) bezpečnost komunikačních sítí
l) aplikační bezpečnost
m) kryptografické algoritmy

LEGISLATIVNÍ RÁMEC OCHRANY OÚ

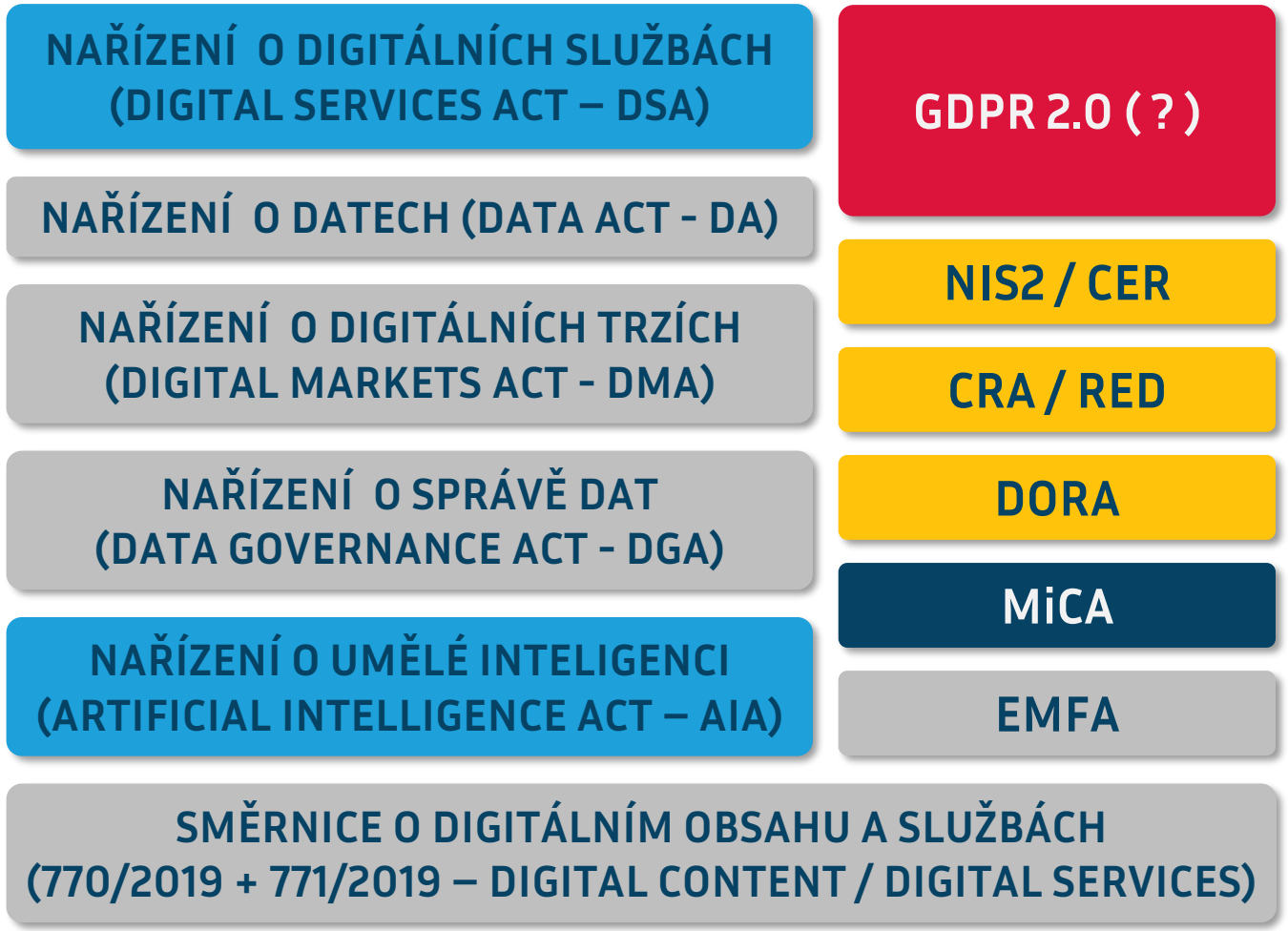
- Evropská digitální strategie (EU Digital Strategy) +
  Evropská strategie kybernetické bezpečnosti (EU Cybersecurity Strategy)

- 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 EDPB
  - > European Data Protection Board (EDPB) → náhrada WP 29
  - > Vodítko k pověřenci pro ochranu osobních údajů (WP 243)
  - > 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 správnímu pokutování (WP 252)

DIGITÁLNÍ DEKÁDA

- Digitální regulaci neutečeme
  - > Digitální strategie EU 2030
  - > Digitální dekáda 2023 – 2026



LEGISLATIVNÍ RÁMEC OCHRANY OÚ

- Obecné právní předpisy
  - Ústava + LZPS
- Z. č. 89/2012 Sb., občanský zákoník
  - § 81 – 90 Ochrana osobnosti a soukromí
- 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
  - Zrušení 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

- Zvláštní právní předpisy →
  > 1 350 předpisů hovoří o ochraně OÚ
  - > Z. č. 262/2006 Sb., zákoník práce + předpisy o zaměstnanosti a o sociální péči
  - > Z. č. 372/2011 Sb., o zdravotních službách + předpisy o ochraně veřejného zdraví
  - > 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, ve znění novely z. č. 374/2021 Sb.
  - > Z. č. 480/2004 Sb., o některých službách informační společnosti
  - > Z. č. 106/1999 Sb., o svobodném přístupu k informacím
  - > Z. č. 181/2014 Sb., o kybernetické bezpečnosti
  - > Z. č. 284/2009 Sb., o platebním styku + předpisy o finančnictví, pojišťovnictví, bankovnictví a obchodování na finančních trzích
  - > Z. č. 280/2009 Sb., daňový řád
  - > Z. č. 256/2013 Sb., katastrální zákon

LEGISLATIVNÍ RÁMEC OCHRANY OÚ

- 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
- Doprovodný změnový zákon
  - Navazuje na návrh ZZOÚ a implementuje směrnice č. 2016/680 a č. 2016/681

MÍSTNÍ A VĚCNÁ PŮSOBNOST GDPR

- 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

- Výluky působnosti GDPR
  - Právnické 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

ZÁKLADNÍ POJMY GDPR

- Meritum
  - > Úpravy
  - > Rozhodovací praxe
  - > Judikatury

OSOBNÍ ÚDAJE PODLE GDPR

- 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*

- Stanovisko WP29 č. 4/2007 k pojmu osobní údaje
  - *Obecně lze fyzickou osobu považovat za „identifikovanou“, jestliže je ve skupině osob „odlišena“ ode všech ostatních příslušníků této skupiny. V souladu s tím je fyzická osoba „identifikovatelná“, jestliže je možné ji identifikovat (přípona „-elná“ vyjadřuje možnost), ačkoli dosud identifikována nebyla.*
  - *Identifikace se obvykle provádí pomocí určitých zvláštních informací, které můžeme nazývat „identifikátory“ a které mají zvláště výsadní a těsný vztah ke konkrétnímu jednotlivci. Patří k nim vnější znaky vzhledu dané osoby, jako je výška, barva vlasů, oblečení atd., nebo vlastnosti osoby, které nejsou bezprostředně vnímatelné, jako je její povolání, funkce, jméno atd.*

OSOBNÍ ÚDAJE PODLE GDPR

- Zákonodárce předpokládá široké pojetí pojmu osobní údaj → „veškeré“
- Použití výrazu „veškeré informace“ v definici pojmu „osobní údaje“ uvedené v tomto ustanovení odráží cíl unijního normotvůrce přiznat tomuto pojmu široký význam, který potenciálně zahrnuje všechny druhy informací, a to jak objektivní, tak subjektivní ve formě názoru nebo hodnocení pod podmínkou, že jsou „o“ dotčené osobě (SDEU C434/16, Peter Nowak)

ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ PODLE GDPR

- 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

- GDPR nestanoví, za jakých okolností se jedná o zvláštní kategorii údajů
  - Musí být takové OÚ skutečně zpracovávány či postačuje možnost z nich údaje vyvodit (vyjma biometrických)?
  - Jakou roli hraje úmysl správce?

ZÁKAZ ZPRACOVÁNÍ ZVLÁŠTNÍCH KATEGORIÍ 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

JUDIKATURA K POJMU OSOBNÍ ÚDAJ

- Judikatura k pojmu a definici OÚ
  - **Rozdíl mezi relativním a objektivním pojetím osobních údajů**
  - Pojetí rozumných prostředků použitých k identifikaci
  - Je relevantní, zda potenciálně identifikující subjekty spolupracují či nikoliv
  - Hranice pojmu zvláštní kategorie osobních údajů
- SDEU
  - C-582/14, Patrick Breyer
  - Tribunál T-557/20, SRB v EDPS
  - C-252/21, Metaplatforms
  - C-184/20, Etikos Komisija
  - C-319/22, GesamtverbandAutoteile-Hande (Scania)
  - C-740/22, Endemol Shine Finland
  - C-479/22 P, OC proti Evropská komise (Europol)
  - C-604/22, IAB Europe
  - C-434/16, Peter Nowak
  - C-372/12, Minister voor Immigratie

JUDIKATURA K POJMU OSOBNÍ ÚDAJ

- Česká judikatura k pojmu a definici OÚ
  - Česká praxe má tendenci zdůrazňovat u identifikovatelnosti osoby objektivní pojetí OÚ
  - Zdrženlivost ohledně toho, co lze považovat za identifikátory

- NSS ČR
  - 1 As 387/2019 SPZ
  - 3 As 76/2022 Spisová značka trestní věci
  - 5 As 158/2012 Identifikátory

JUDIKATURA K POJMU ZVLÁŠTNÍ KATEGORIE OÚ

- Judikatura k pojmu a definici zvláštních kategorií OÚ

- SDEU
  - C-252/21 – Metaplatforms
  - C-184/20 – Etikos Komisija
  - C-184/20 – ND v. DE (*Lindenapotheke*)

DOPADY JUDIKATURY

- Velké množství praktických problémů
  - Absolutní a relativní pojetí – hodnocení subjektivní identifikovatelnosti z pohledu osoby, jež má údaje k dispozici
  - Identifikovaná × identifikovatelná osoba
  - Míra identifikovatelnosti osoby → kdy se vlastnosti skupiny osob přenášejí na všechny členy – tzv. k-anonymita (C-300/21, Österreichische Post)
  - Jak zohlednit přístup založený na riziku
  - Identifikovatelnost × koncept *singling out*
  - Kontextové informace nutné pro správnou interpretaci údajů jako osobní údaje (SDEU C-434/16, Peter Nowak, C-141/12 a C-372/12, Minister voor Immigratie)

DOPADY JUDIKATURY

- Pojem *osobní údaj* ve smyslu vyplývajícím z judikatury
  - Objektivní informaci či subjektivní názor (SDEU, C-434/16, Peter Nowak)
  - Údaje týkající se soukromí či pracovní činnosti
  - Pravdivé či nepravdivé údaje (obvykle)
  - Nerozhoduje forma zaznamenání či předání informace (pokud bude naplněn čl. 2 GDPR) (SDEU C-740/22)
  - O jaký druh údaje se bude jednat
  - Pro postavení správce není rozhodné, zda má osobní údaje k dispozici či nikoliv (SDEU C-25/17 – Svědkové Jehovovi)

- Stanovisko WP29 5/2014 k technikám anonymizace

VYBRANÉ DEFINICE GDPR

- 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

- 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*
- 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

VYBRANÉ DEFINICE GDPR

— 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*

PRÁVNÍ TITULY ZPRACOVÁNÍ OÚ

- 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
    → Pokyny EDPB č. 5/2020 k souhlasu podle nařízení 2016/679

- SDEU
  - > Spojené věci C-468/10 a C-469/10, ASNEF a FECEMD
  - > C-26/22 a C/64/22, SCHUFA Holding
  - > C-621/22, Nederlandse Lawn Tennisbond

BALANČNÍ TEST

- Pokud **správce** zpracovává osobní údaje na základě oprávněného zájmu (čl. 6 odst. 1 písm. f) GDPR), **musí nejdříve vyhodnotit, zda nad jeho oprávněným zájmem nepřevažují zájmy subjektu osobních údajů**
  - Správce musí posoudit přiměřenost jeho oprávněného zájmu vzhledem k právům a zájmům subjektu → **balanční test (test proporcionality)**
  - Provádí se ještě **před zahájením zpracování**
- Pokud je výsledek testu pozitivní, tj. oprávněný zájem správce je vyšší než práva subjektu, může osobní údaje zpracovávat na základě právního důvodu
  - Informační povinnost vůči subjektu
  - Informace o tom, v čem spočívá jeho oprávněný zájem
- V opačném případě by nemělo ke zpracování vůbec docházet, ledaže je zde jiný právní titul

BALANČNÍ TEST

- Stanovisko ÚOOÚ (závěry kontrolních akcí 2019)

  Musí správce vždy provádět balanční test v případě zpracování osobních údajů prováděného na základě oprávněného zájmu?

  Správce je povinen provést balanční test, neboli test proporcionality, pro každé zpracování osobních údajů, které hodlá vykonávat na základě právního důvodu oprávněného zájmu. *Balanční test by měl být vypracován ve vztahu k účelu zpracování, přičemž pro obdobné účely postačuje vypracování jednoho balančního testu.* ***Právě v důsledku takového testu*** *je pak správce schopen vyhodnotit, zda před jeho oprávněnými zájmy nemají přednost zájmy nebo práva a svobody subjektu údajů, a* ***lze tak tento právní důvod pro zpracování osobních údajů využít****.*

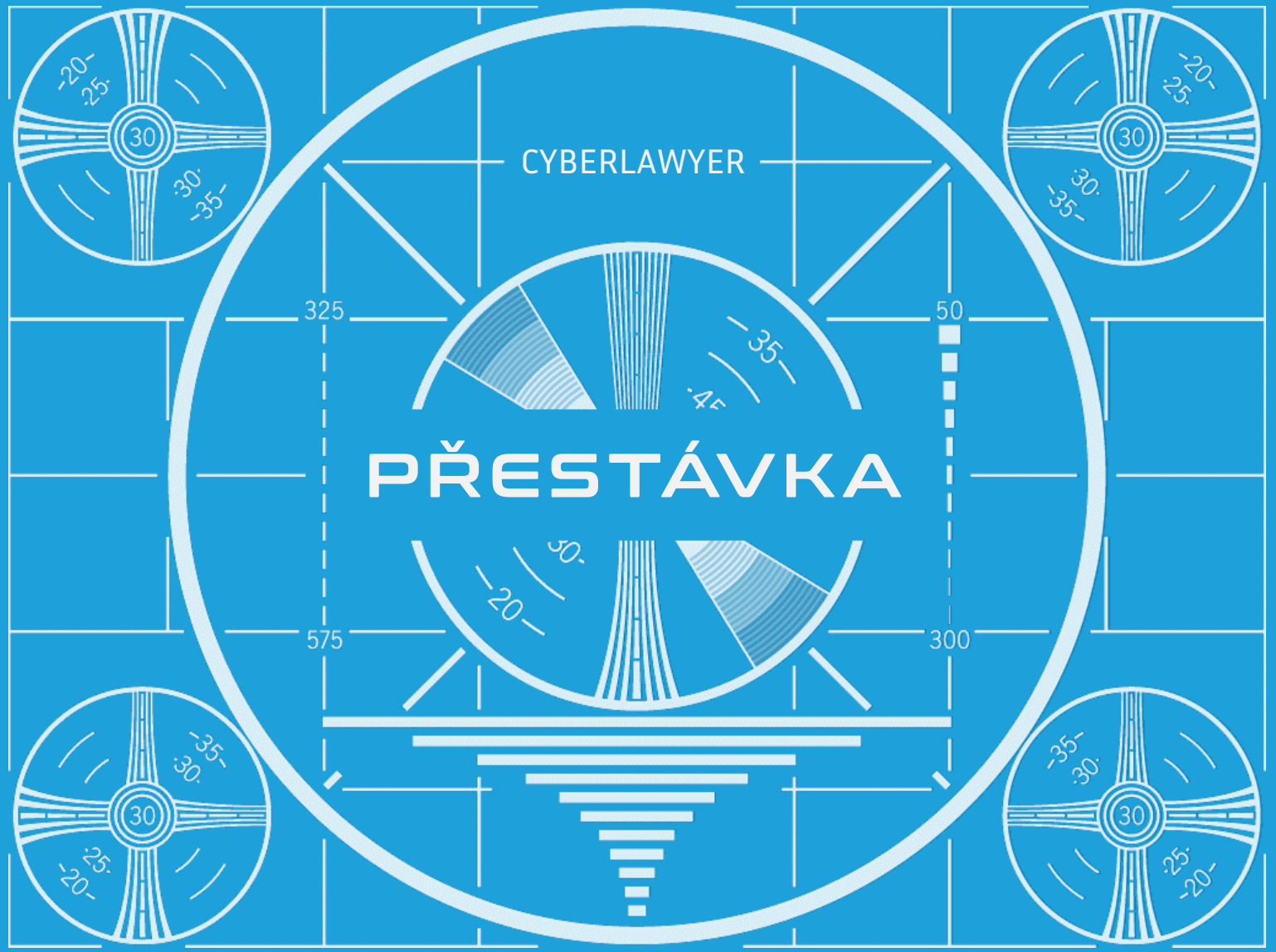
  V rámci tohoto posouzení (balančního testu) ***je nutné vzít do úvahy více faktorů, a to především váhu samotného oprávněného zájmu, možné negativní či pozitivní důsledky pro subjekty údajů, rozumné očekávání subjektů údajů ohledně zpracování či vztah správce a subjektu údajů****. I výsledek balančního testu lze nakonec ovlivnit ve prospěch správce také přijetím vysokých záruk bezpečnosti zpracování či vyšší transparentností zpracování. Posouzení oprávněného zájmu je zároveň nutné* ***pečlivě dokumentovat*** *a být připraven jej v souladu se zásadou odpovědnosti předložit ÚOOÚ ke kontrole.*

BALANČNÍ TEST

- Typické situace zpracovávání osobních údajů na základě oprávněného zájmu
  - Ochrana zdraví a majetku
  - Sledování zaměstnanců pro účely bezpečnosti a řízení
  - Zamezení podvodům
  - Zabezpečení IT systémů a kybernetická bezpečnost
  - Přímý marketing (zasílání newsletterů)
  - Trénink a využití nástrojů umělé inteligence (AI) (?)

BALANČNÍ TEST

- Obsah
  - Význam oprávněného zájmu správce
  - Hrozící riziko pro subjekt osobních údajů, jehož OÚ jsou správcem zpracovávány
  - Očekávání subjektu při zpracovávání jeho OÚ
  - Míru bezpečnostních opatření
  - Vyhodnocení
- Forma
  - GDPR formu nestanoví
  - V případě kontroly je nutné vypracování tohoto testu doložit
    → **provedení balančního testu písemně**


CYBERLAWYER
PŘESTÁVKA
325
50
575
300

VYBRANÉ POVINNOSTI REGULOVANÝCH SUBJEKTŮ

- Vedení záznamů o činnostech zpracování, jejich využití a údržba v praxi
- Tvorba hodnocení dopadů (DPIA, TIA, FRIA)
- Interní bezpečnostní opatření
- Reakce na bezpečnostní incident v oblasti zpracování OÚ

DESATERO GDPR COMPLIANCE (7+3)

- Aktuální dokumentace naplňování zásad zpracování, ochrany a zabezpečení OÚ dle čl. 5, 6, 25 a 32 GDPR
- Aktuální záznamy o zpracování OÚ dle čl. 30 GDPR
- Naplňování informační povinnosti vůči subjektům údajů dle čl. 12 – 14 GDPR
- Proces naplňování práv subjektů údajů dle čl. 15 – 24 GDPR a vedení jejich evidence
- Proces identifikace, vyhodnocení a hlášení bezpečnostních incidentů a vedení jejich evidence
- Revize a renegociace smluv → smlouvy o zpracování OÚ dle čl. 28 GDPR
- Systém evidence souhlasů subjektů se zpracováním OÚ

- Ustavení a zajištění funkce DPO
- Provedení posouzení vlivů na zpracování OÚ (DPIA)
- Pravidelné zlepšování, zajišťování awareness a testování prostředí

GDPR COMPLIANCE REPOSITORY

- Nástroj pro prokazování compliance
  - Zásada odpovědnosti
  - Zásada přístupu založeného na řízení rizika
- Forma
  - Elektronická dokumentace (uložiště) ×
  - Fyzický otisk (šanon) ×
  - Kombinace
- Obsah
  - Souhrnná auditní / analytická zpráva
  - Záznamy o činnostech zpracování
  - Balanční testy
  - Vnitřní normy a řídící dokumentace
  - Dokumentace informační povinnosti vůči subjektům údajů
  - Dokumentace práv subjektů údajů
  - Smlouvy o zpracování OÚ
  - Procesy identifikace a hlášení bezpečnostních incidentů
  - Záznamy o DPIA

DOKUMENTACE NAPLŇOVÁNÍ ZÁSAD GDPR

- Dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení OÚ
  - Nejméně čl. 5, 6, 9, 25 a 32 GDPR
  - Zásady odpovědnosti a přístupu založeného na řízení rizika
- Obsah
  - Stručný popis prostředí a procesů správce ve vztahu ke zpracování OÚ
  - Identifikace hlavních skupin subjektů údajů
    - Klienti, protistrany a zástupci, účastníci řízení, zaměstnanci, apod.
  - Popis hlavních oblastí (domén) zpracování OÚ
    - Klientská dokumentace, pracovněprávní a mzdová agenda, účetní a daňová agenda apod.
  - Identifikace kritických anebo nepokrytých míst z pohledu naplnění zásad zpracování a ochrany OÚ a jejich rizikovosti
    - Klientská dokumentace
    - Zabezpečení OÚ
    - Zvláštní kategorie OÚ
  - Popis přijatých organizačních a technických opatření k dosažení shody

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

- Výslovně definovaná povinnost vést záznamy o činnostech zpracování
  - Record of Processing Activities (ROPA)
  - Čl. 30 a násl. GDPR

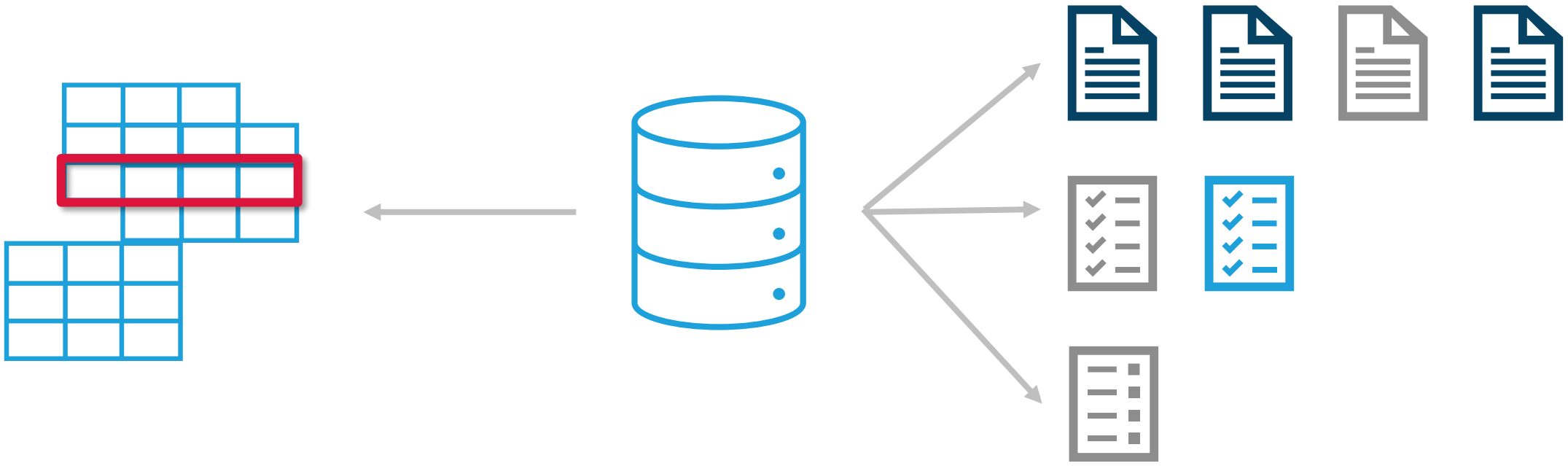
- Písemné záznamy, dostupné na vyžádání dozorovému úřadu
  - Povinná písemná forma → GDPR nedefinuje způsob pořízení a zpracování
  - Výjimka pro malé a střední podniky do 250 zaměstnanců (?)

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

- Správce je povinen doložit, že:
  - Zpracování je prováděno v souladu s nařízením
  - Opatření jsou aplikována v souladu s nařízením (zákonem)
  - Opatření jsou podle potřeby revidována a aktualizována
  - Při tvorbě opatření zohlednil
    - Povahu, rozsah, kontext a účely zpracování
    - Různě pravděpodobná a různě závažná rizika pro práva a svobody fyzických osob (*risk-based approach*)

- Minimální obsah
  - Procesní přístup × Objektový přístup (přes evidence)
  - Evidence / Proces
  - Kategorie osobních údajů
  - Subjekt osobních údajů
  - Účel a právní základ (titul) zpracování
    → **pozor na souhlas / oprávněný zájem**
  - Druh a forma zpracování
  - Kompetentní osoby
  - Předávání třetím osobám, popř. do zahraničí
  - Základní *risk-assessment*

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ



Strukturovaná evidence (Tabulka)

Databáze zpracování (Data Inventory)

Nestrukturovaná evidence (Popisy procesů a karty)

NAPLŇOVÁNÍ PRÁV SUBJEKTŮ

- I při výkonu advokacie mají subjekty údajů svá práva podle 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

- 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

- 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

DALŠÍ PRÁVA SUBJEKTŮ ÚDAJŮ

- 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 ÚDAJŮ

- 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**

DALŠÍ PRÁVA SUBJEKTŮ ÚDAJŮ

- Čl. 17 GDPR – Právo subjektu na vyžádaný výmaz jeho OÚ

- 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 ÚDAJŮ

- 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 namítajícího
  - > 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

POSOUZENÍ VLIVŮ NA ZPRACOVÁNÍ OÚ (DPIA)

- Čl. 35 – 36 GDPR
  - Recitály: 84, 89 – 95
  - Vodítko WP 29 (WP 248)
  - Provádí zásadu odpovědnosti a částečně nahrazuje registrační povinnost
- Povinnost provést posouzení vlivu na ochranu OÚ (*DPIA*)
  - Každé stávající nebo připravované zpracování OÚ → doporučeno i pro současné operace
  - Posouzení vlivu konkrétních operací při **procesech zpracování OÚ, které představují nebo mohou představovat vysoké riziko pro práva a svobody FO**
  - Pokud je identifikováno vysoké riziko, které nelze eliminovat →
- Povinnost předchozí konzultace s dozorovým úřadem

POSOUZENÍ VLIVŮ NA ZPRACOVÁNÍ OÚ (DPIA)

- DPIA **je nutné**
  - Systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování → **AI**
    - Včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k FO právní účinky nebo mají na fyzické osoby podobně závažný dopad
  - Rozsáhlé zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se trestních věcí
  - Rozsáhlé systematické monitorování veřejně přístupných prostorů
    - Např. instalace kamerového systému
- DPIA **není nutné**
  - Pokud zpracování OÚ nepředstavuje vysoké riziko
  - Pokud již bylo DPIA provedeno pro velmi podobné zpracování
  - Pokud se jedná o zpracování na základě právní povinnosti mající základ v unijním právu nebo právu členského státu EU
  - Pokud je zpracování uvedeno na seznamu zpracování, které nevyžadují DPIA (seznam vypracovaný ÚOOÚ)

POSOUZENÍ VLIVŮ NA ZPRACOVÁNÍ OÚ (DPIA)

- DPIA obsahuje alespoň
  - Popis zamýšlených operací zpracování a účely
  - Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu
  - Posouzení rizik pro práva a svobody subjektů údajů
  - Plánovaná opatření k řešení těchto rizik (záruky, bezpečnostní opatření, mechanismy k zajištění ochrany a doložení souladu s GDPR)
  - Zohlednění dodržování kodexů chování
- Přezkum s cílem posoudit, zda je zpracování prováděno v souladu s DPIA
  - Při změně rizika – průběžně

KDY JE VHODNÉ PROVÉST DPIA?

1. Nasazení nového IT systému, který také ukládá nebo zpracovává osobní údaje → AI
2. Sdílení údajů mezi dvěma organizacemi
3. Návrh vybírat lidi z určité množiny a iniciovat vůči nim nějakou akci (typicky marketing)
4. Použití existujících dat pro nové účely (zvláště jsou-li pro lidi víc rušivé)
5. Nový monitorovací systém (zejména zahrnuje-li i část veřejnosti) nebo použití nové technologie v existujícím systému (např. rozpoznávací technologie v CCTV) → AI
6. Nová databáze, která shromažďuje informace, které už v různých částech organizace existují
7. Legislativa, politika nebo strategie, která může mít dopad na soukromí v důsledku používání informací nebo monitorováním → AI

PŘESHRANIČNÍ ZPRACOVÁNÍ OÚ V RÁMCI EU

- Předávání OÚ v rámci EU → svoboda pohybu osobních údajů ×
  - Předávání OÚ do třetích zemí nebo mezinárodním organizacím
- Přeshraniční zpracování
  - Správce / zpracovatel je usazen ve více než jednom členském státě + zpracování probíhá v souvislosti s činnostmi provozoven ve více než jednom státě EU
  - Zpracování OÚ, které probíhá v souvislosti s činnostmi jediné provozovny správce / zpracovatele v EU, kterým jsou nebo budou podstatně dotčeny subjekty údajů ve více státech

PŘESHRANIČNÍ ZPRACOVÁNÍ OÚ MIMO EU

- Obecná zásada bezpečnosti zpracování
  - K předání OÚ může dojít pouze tehdy, splní-li správce/zpracovatel podmínky GDPR
  - Cílem úpravy předání OÚ **zajistit, aby úroveň ochrany FO zaručená GDPR nebyla snížena**
- 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

- Schrems II
  - Rozsudek Soudního dvora (velkého senátu) ze dne 16. července 2020 ve věci C-311/18 – *Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems*
  - Žádost o rozhodnutí o předběžné otázce podaná irským High Court především ve věci předávání osobních údajů do třetích zemí pro obchodní účely
- Vývozce osobních údajů musí předem každého exportu mimo EU posoudit, zda:
  - Odesílá osobní údaje mimo EU? Pokud ano, jaké, v jakém rozsahu a komu?
  - Jaké zabezpečení je zavedeno v souvislosti s předáváním a zpracováním údajů (zde v USA)?
  - Je ve státě importu osobních údajů zavedena úroveň ochrany odpovídající GDPR?
- Posouzení vlivů předání na zpracování OÚ – *Transfer Impact Assessment* (TIA)

TRANSFER IMPACT ASSESSMENT (TIA)

- Posouzení vlivu předávání údajů (TIA)
  - Objasňuje rizika při předávání údajů obyvatel EU do zemí, které nemají odpovídající úroveň ochrany osobních údajů podle GDPR
  - Proces vyhodnocení potenciálních dopadů přenosu osobních údajů z jedné jurisdikce nebo místa do druhého
  - Účelem identifikovat potenciální rizika a přínosy přenosu osobních údajů
    - Jak může ovlivnit různé zúčastněné strany?
    - Jak může ovlivnit širší systém správy osobních údajů?
    - Jak budou osobní údaje chráněny na základě zákonů na ochranu údajů přijímající země? Nepředstavuje to průlom anebo snížení standardu ochrany osobních údajů?

TRANSFER IMPACT ASSESSMENT (TIA)

- **Kdy je TIA nutná?**
  - Pro každou novou činnost zpracování, která zahrnuje předávání údajů do zemí mimo EHP a pro kterou současně EK nevydala rozhodnutí o shodné míře ochrany (*adequacy resolution*)
  - Pro podstatné změny stávajících činností zpracování,
    které nově zahrnují předávání údajů do zemí mimo EHP
- **Case-by-case!**
- Přínosy posouzení dopadů předávání
  - Zajištění souladu s GDPR a zmírnění rizik spojených s předáváním údajů před zahájením předávání / zpracování
  - Určení pravděpodobnosti žádostí o přístup ze strany státních orgánů v zemi dovozu / třetí zemi
  - Identifikace kroků pro efektivní zmírnění rizik ještě před zahájením zpracování
  - Povědomí o právních předpisech a postupech v oblasti ochrany údajů v dovážející zemi / třetí zemi
  - Úspora času a nákladů na případné správní sankce, náklady za právní služby a poplatky
  - Soulad s výsledky rozhodnutí Schrems II a požadavky obecné compliance v oblasti ochrany osobních údajů

POVĚŘENEC PRO OCHRANU OÚ (DPO)

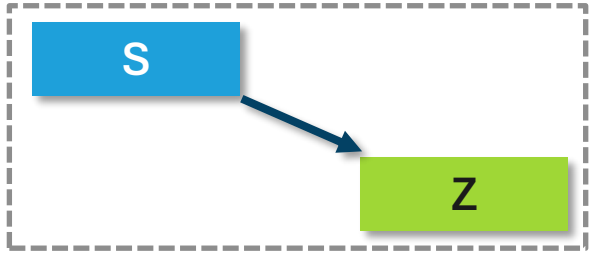
- Čl. 37 až 39 GDPR + recitály 77 a 97
  - Vodítko WP 29 k pověřencům pro ochranu OÚ (WP 243 rev.01)
  - Zákon o zpracování OÚ (zejm. § 12, § 13)
  - Doprovodný zákon k zákonu o zpracování OÚ
- Kdo musí jmenovat pověřence?
  - Každý orgán veřejné moci nebo veřejný subjekt
  - Subjekty provádějící v rámci 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
  - Dobrovolné jmenování
    - DPO pak podléhá stejným povinnostem jako u povinně jmenovaného

ÚKOLY DPO

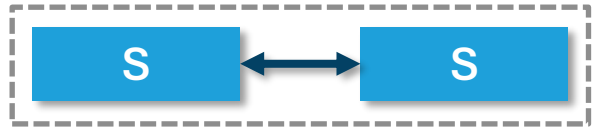
- Primární úkoly DPO (čl. 39 GDPR)
  - Monitorování zpracování OÚ s cílem zajistit soulad s GDPR
  - Zajišťování provádění práv subjektů údajů
  - Evidenční a reportovací činnost DPO
  - Posuzování vlivu na zpracování OÚ (DPIA, konzultace s ÚOOÚ)
  - Ohlašování a řešení bezpečnostních incidentů
  - Spolupráce s ÚOOÚ
  - Konzultace a odborná vyjádření uvnitř organizace i navenek
  - Vzdělávání a školení zaměstnanců, případně externích dodavatelů
- Součástí všech úkolů pravidelný risk-assesment a vyhodnocování požadavků ochrany a zabezpečení OÚ

SMLOUVY O ZPRACOVÁNÍ OÚ

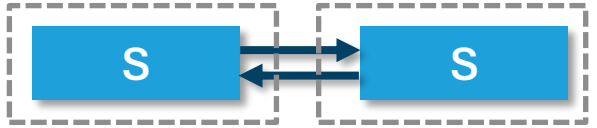
- Smlouva o zpracování osobních údajů
  - Čl. 28 GDPR → minimální obsah v odst. 3
  - Smlouva mezi správcem a zpracovatelem



- 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 OÚ

- 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 → čl. 28 odst. 3 GDPR
  - Předmět a doba trvání zpracování
  - Povaha a účel zpracování
  - Typ OÚ a kategorie subjektů údajů
  - Povinnosti a práva správce

SPRÁVA OÚ PŘI VÝKONU ADVOKACIE

- Správce vs. zpracovatel
  - Advokát je správcem osobních údajů klientů, protistran, svědků i zaměstnanců.
  - **Může být advokát zpracovatelem?**

- Zpracování údajů jen v nezbytném rozsahu a s právním základem
  - Každé zpracování musí být nezbytné pro výkon advokacie (plnění smlouvy, právní povinnost, oprávněný zájem, výkon obhajoby)
  - Zásada minimalizace údajů
  - Při práci s citlivými údaji (např. zdravotními či trestními) je nutné zajistit zvláštní ochranu podle čl. 9 a 10 GDPR

SPRÁVA OÚ PŘI VÝKONU ADVOKACIE

- Zachování mlčenlivosti = zachování ochrany a bezpečnosti OÚ
  - Povinnost advokátní mlčenlivosti doplňuje a zpřísňuje bezpečnostní požadavky GDPR
  - Nutnost implementace technických a organizačních opatření: šifrování, silná autentizace, bezpečné e-maily, fyzická kontrola přístupu
  - Povinnost zajistit, že všichni zaměstnanci a spolupracovníci dodržují mlčenlivost i po skončení spolupráce

- Transparentní a řízená správa dokumentů a komunikace
  - Zavedení systému evidence a uchovávání spisů v souladu se zákonem o advokacii a GDPR
  - Oddělení spisové agendy (klienti, interní věci, personalistika)
  - Používání bezpečných komunikačních kanálů a řízené mazání dat po uplynutí retenčních lhůt

SPRÁVA OÚ PŘI VÝKONU ADVOKACIE

- Prokazatelnost a odpovědnost (accountability)
  - > Vedení záznamů o činnostech zpracování (ROPA) i v menších kancelářích – důkaz řádného řízení údajů
  - > Pravidelné interní kontroly a školení zaměstnanců o ochraně osobních údajů
  - > Připravenost na incidenty a žádosti subjektů údajů – jasné postupy, kdo a jak reaguje

PROČ TOMU MÁME VĚNOVAT POZORNOST?

SPRÁVNÝ PŘÍSTUP

Přinejmenším minimální GDPR compliance (7+3)

- Rozumná aplikace požadavků s přihlédnutím k prostředí, potřebám a možnostem organizace a jejímu rizikovému profilu
- Integrace do všech procesů a evidencí organizace (i kdyby postupná)
- Zásady ochrany a zabezpečení OÚ
- DPIA

Řízené pravidelné zlepšování

- *Tone from the Top*
- Vzdělávání a zvyšování risk-awareness

TYPICKÉ RIZIKOVÉ SCÉNÁŘE

Potěmkinova vesnice

Dělo na vrabce

Spekulativní ignorace regulace / Rezignace

TYPICKÉ APLIKAČNÍ PROBLÉMY

Chybějící reflexe principů ochrany a zabezpečení OÚ

Nedostatečná dokumentace shody

Nedostatečná příprava a implementace prostředí, procesů a opatření

Smlouvy o zpracování OÚ a další smluvní vztahy související s nakládáním s informacemi

ZNÁMÉ VÝZVY

- Souběh GDPR a dalších předpisů
  - > Principy ochrany a zabezpečení OÚ zůstávají jádrem compliance s datovými regulacemi
  - > GDPR je horizontální norma, kdežto větší část předpisů Digitální dekády je sektorových
  - > Povinnost sladit bezpečnostní, informační a etické požadavky napříč množstvím regulací
    → chybí mapování a aplikační vodítka

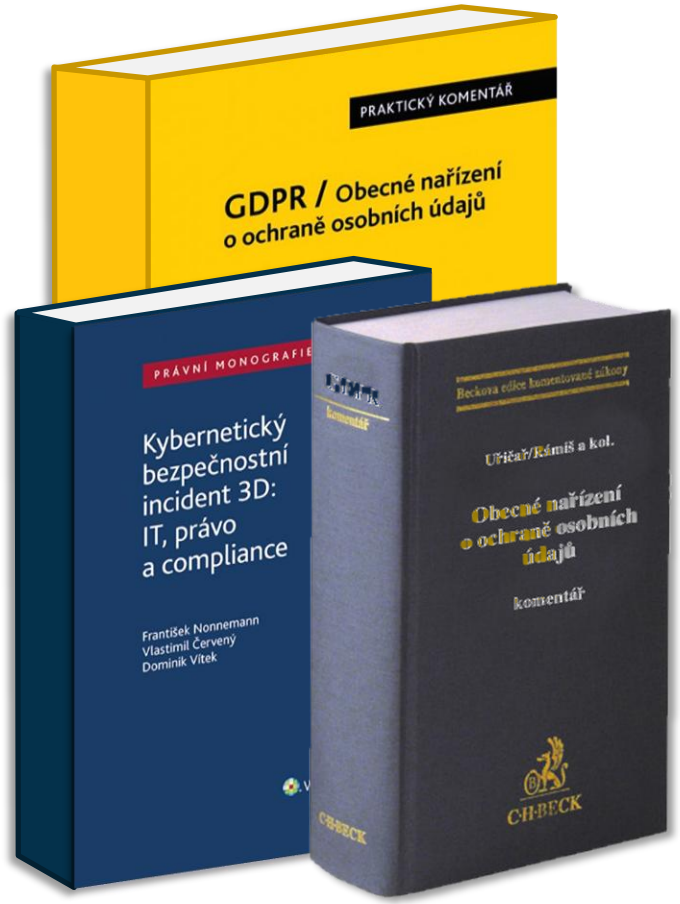
- Při implementaci vždy vznikají neočekávané překryvy, konflikty a duplicity
  - > GDPR vs. NIS2, CER a DORA – ochrana soukromí vs. požadavky na monitoring a kontrolu uživatelů
  - > GDPR vs. DA – sdílení vs. omezení z důvodu ochrany osobních údajů
  - > GDPR vs. AIA – rozhodování bez lidského zásahu vs. informace o zpracování OÚ
  - > GDPR vs. DSP– moderace, reklama a targeting

ZNÁMÉ VÝZVY

- Aplikační problémy
  - Upřednostňování jedné regulace před ostatními
  - Přílišné spoléhání na jednu roli nebo dokumentaci k jedné z regulací
  - Nedostatečná koordinace mezi DPO, CISO/CTO/CIO a právním týmem

- Doporučení pro organizace
  - Regulace ochrany OÚ, AI a IKB jsou propojené nádoby (či různé strany téže kostky) →
  - Interní principy, politiky a odpovědnosti v oblasti zpracování dat, AI a kyberbezpečnosti revidujte vždy společně
  - Zmapujte dopady nových regulací na datové toky, informační systémy a datové smlouvy
  - Vytvořte koordinační mechanismus mezi právním týmem / compliance, DPO, CISO / CIO a AI governance týmem
  - Podporujte tvorbu a sdílení kompetencí – školení, interdisciplinární workshopy

LITERATURA A ONLINE ZDROJE



- NULÍČEK, M., DONÁT, J., NONNEMANN, F. a kol. GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář. 2., aktualizované vydání. Praha : Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.

- UŘIČAŘ, M., RÁMIŠ, V. a kolektiv. Obecné nařízení o ochraně osobních údajů. Komentář. Praha : C.H.Beck, 2020. ISBN 978-80-7400-815-3.

- NONNEMANN, František, Vlastimil ČERVENÝ a Dominik VÍTEK. Kybernetický bezpečnostní incident 3D: IT, právo a compliance. Praha: Wolters Kluwer, 2022. ISBN 978-80-7676-515-3.

LITERATURA A ONLINE ZDROJE

- Právní předpisy
  - Obecné nařízení o ochraně osobních údajů
  - Čl. 25 a 32, 30, 33 – 34, 35, 37 – 39 a 44 – 50

  - Zákon č. 110/2019 Sb., o zpracování osobních údajů, v aktuálním znění
    - Hlava V (právní zakotvení činnosti ÚOOÚ)

LITERATURA A ONLINE ZDROJE

- Pokyny a doporučení Evropského sboru / inspektora pro ochranu osobních údajů (EDPB / EDPS)
  - Dostupné na stránkách EDPB
  - Pokyny 04/2019 Čl. 25 a principům záměrné a standardní ochrany osobních údajů
  - Pokyny 01/2021 Příklady ohlašování případů porušení zabezpečení osobních údajů
  - Pokyny 04/2022 k výpočtu správních pokut podle GDPR
  - Pokyny 09/2022 k hlášení bezpečnostních incidentů na poli ochrany osobních údajů (personal data breach)
  - Doporučení 01/2019 k návrhu seznamu evropského inspektora ochrany údajů, pokud jde o operace zpracování, na něž se vztahuje požadavek na posouzení vlivu na ochranu osobních údajů (čl. 39 odst. 4 nařízení (EU) 2018/1725)

LITERATURA A ONLINE ZDROJE

- Stanoviska pracovní skupiny WP29
  - Dostupné na stránkách EDPB
  - Stanovisko WP29 Posouzení vlivu na ochranu osobních údajů a vysoce rizikové zpracování osobních údajů
  - Stanovisko WP29 Ohlášení případů porušení zabezpečení osobních údajů
  - Stanovisko WP29 Pověřenec pro ochranu osobních údajů
- Metodiky ICO
  - Provádění DPIA

DISKUSE (Q&A)

DOTAZY?
PŘÍPOMÍNKY?
NADŠENÍ? ZKLAMÁNÍ?

Jindřich Kalíšek
advokát

kalisek@cyberlawyer.cz
kalisek@regfor.cz