Příprava na GDPR krok za krokem

6. prosince 2017, Brno

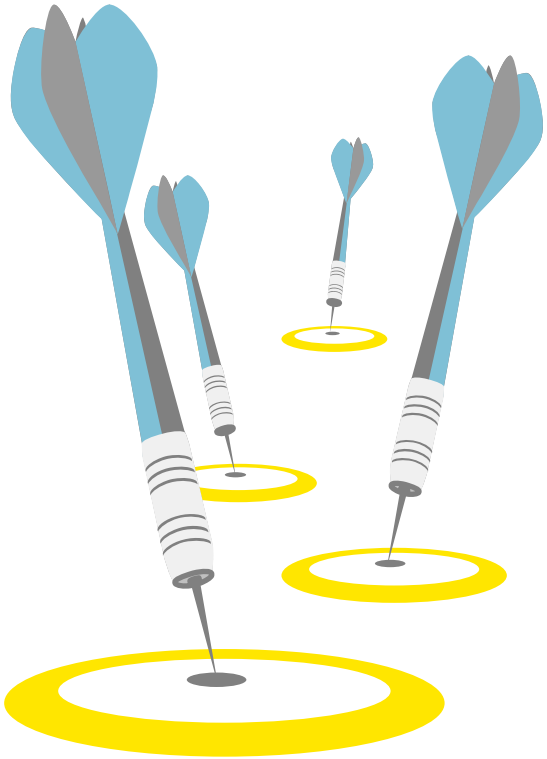
FORUM

Naše znalosti
pro Váš úspěch

Weinhold Legal

Program

1. Nová úprava v oblasti ochrany osobních údajů
2. Zpracování osobních údajů – základní pojmy a zásady
3. Povinnosti správce
4. Pověřenec pro ochranu osobních údajů
5. Posílení práv subjektů údajů
6. Předávání osobních údajů
7. Orgány ochrany osobních údajů
8. Sankce
9. Jak se nachystat na GDPR



1. Nová úprava v oblasti ochrany osobních údajů

Na úvod – stávající právní úprava

- Zákon č. 101/2000 Sb., o ochraně osobních údajů
  - základní zásady: legalita a legitimita, přiměřenost, účelovost
  - informační povinnost správce
  - zpracování na základě souhlasu či dalších zákonných důvodů
  - oznamovací povinnost ohledně zpracování vůči ÚOOÚ
  - povolovací řízení v případě předání osobních údajů do třetích zemí
  - mírnější sankce (max. 10 milionů Kč)

Obecné nařízení o ochraně osobních údajů (GDPR)

- 3 důvody přijetí GDPR
  - vývoj v oblasti zpracování osobních údajů
  - zastaralost směrnice 95/46/ES
  - sjednocení v rámci EU a EHP
- **Časová působnost**: od **25.5.2018** plně použitelné
- **Osobní působnost**: subjekt nakládající s údaji občanů EU
- **Místní působnost**: univerzální
- **Věcná působnost**:
  - věrnostní programy, zákaznické údaje, zaměstnanecké údaje
  - platební informace
  - distribuce přes internet
  - retail
  - veřejný sektor atd.

Další relevantní právní předpisy

- Nařízení o soukromí a elektronických komunikacích (**ePrivacy nařízení**)
  - schváleno již Evropským parlamentem, plánovaná účinnost společně s GDPR
- **Nový zákon o zpracování osobních údajů**
  - aktuálně v připomínkovém řízení
  - má zrušit zákon č. 101/2000 Sb., o ochraně osobních údajů
  - navrhovaná účinnost společně s GDPR
  - implementace některých místních specifik dle GDPR a sankční směrnice 2016/680
- Prováděcí novela k zákonu o zpracování osobních údajů

Hlavní novinky v GDPR I.

Rozšířená působnost

- Všichni správci a zpracovatelé osobních údajů **v EU** a ti, kteří cílí na **občany EU** (tedy i správci a zpracovatelé mimo EU)

Povinnosti správců/ zpracovatelů

- Posoudit **vlivy zpracování na ochranu OÚ** před započetím zpracování **(analýza rizik)**
- **Zabezpečit soulad s GDPR** - dokumentovat zásady zpracování údajů, procesy a operace, a zpřístupnit je na žádost dozorujícímu úřadu – **záznamy o zpracování OÚ, nebo kodexy, certifikace**
- **Rozšíření informační povinnosti**
- **Ohlašovací** a **oznamovací povinnost** při porušení zabezpečení OÚ
- Pseudonymizace OÚ
- **Konzultační** povinnost vůči ÚOOÚ (odpadá registrace)
- Ustavení **pověřence pro ochranu OÚ**
- **Posílení odpovědnosti zpracovatelů**

Hlavní novinky v GDPR II.

Posílení práv subjektů údajů

- Výslovná úprava práva být **zapomenut**
- Právo **vznést námitku**
- Právo na **přenositelnost údajů**

Souhlas

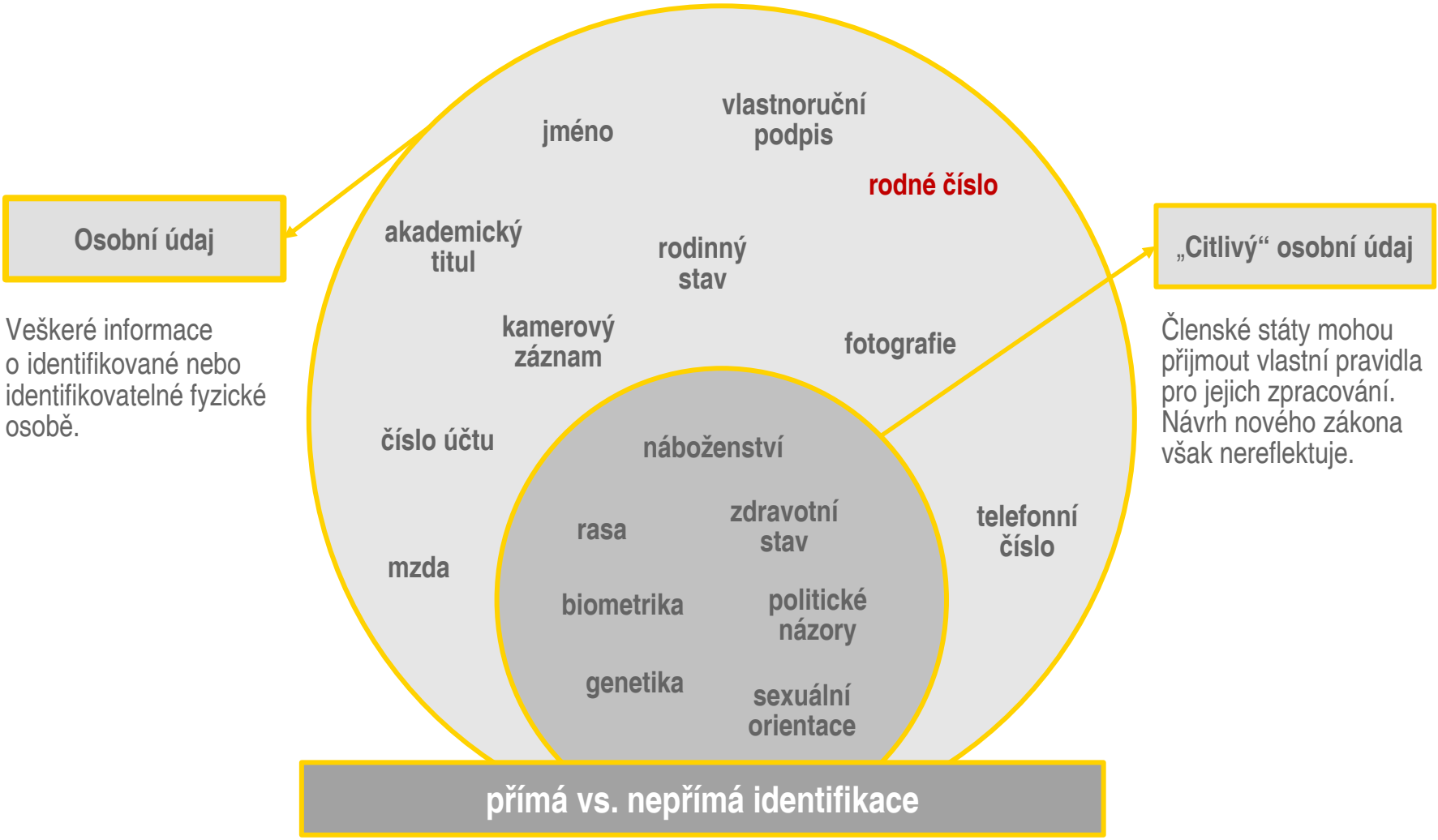
- Musí být dán svobodně a pro **vymezené účely**
- Správce musí informovat subjekt o **právu vzít souhlas zpět**
- Souhlas musí být **„výslovný“, odlišitelný**
- **Přechod stávajících souhlasů**, pokud splňují náležitosti dle GDPR x **jinak potřeba revize**

Sankce

- Pokuty za porušení GDPR jsou astronomické
- Úřady mohou uložit pokuty až do výše **4 % ročního celosvětového obratu** nebo **20 mil. €**, podle toho, co je vyšší

2. Zpracování osobních údajů – základní pojmy a zásady

Subjekt údajů, osobní údaje a zvláštní kategorie osobních údajů



Zpracování osobních údajů

Jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn pomocí či bez pomoci automatizovaných postupů

Kdo je kdo?

Správce

- Osoba (FO/PO), která sama nebo společně s jinými určuje účel a prostředky zpracování osobních údajů
- Např. zaměstnavatel, banka, společnost vedoucí databázi klientů

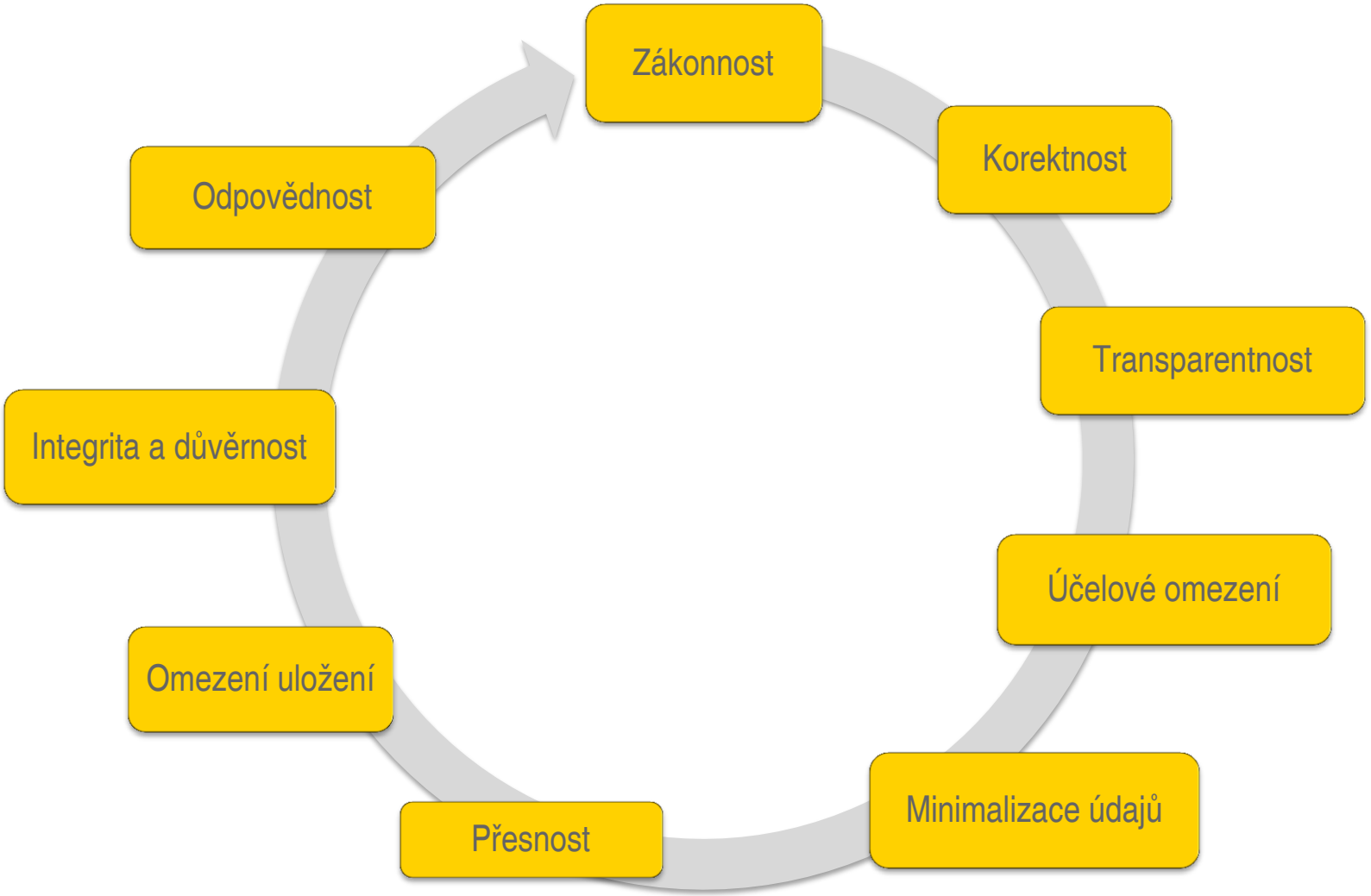
Zpracovatel

- Osoba (FO/PO), která zpracovává osobní údaje pro správce

Příjemce

- Osoba (FO/PO), které jsou osobní údaje poskytnuty
- Tj. subjekt údajů, zpracovatel, jiný správce, třetí strana

Základní zásady zpracování



Zásada odpovědnosti

Princip „odpovědnosti“

- Převzetí odpovědnosti vyžaduje **implementaci opatření** pro zvýšení a **zajištění ochrany osobních údajů v průběhu jejich zpracování (například minimalizace údajů).**
- Zpracovatelé jsou odpovědní za soulad procesu zpracování osobních údajů s právním rámcem.
- Zpracovatelé mají povinnost udržovat **aktuální dokumentaci** za účelem **demonstrace souladu** s předpisy pro ochranu osobních údajů pro veřejnost i dohlížející orgány.

Přijetí směrnic a implementace příslušných opatření pro **zajištění zabezpečení osobních údajů v průběhu celého životního cyklu**

Řízení životního cyklu osobních údajů

Weinhold Legal

Kdy mohu osobní údaje zpracovávat? (Právní titul pro zpracování)

1. Pro účely smlouvy uzavřené se subjektem údajů

2. Pro plnění právní povinnosti správce

3. Pro ochranu životně důležitých zájmů subjektu údajů nebo jiné osoby

4. Pro splnění úkolu správce ve veřejném zájmu nebo při výkonu veřejné moci

5. Pro účely oprávněných zájmů správce či třetí strany

6. Se souhlasem subjektu údajů

1. Smlouva

Zpracování je nezbytné:

1. Pro uzavření smlouvy, jejíž stranou je subjekt údajů
   - typicky identifikační údaje
2. Pro plnění závazku ze smlouvy uzavřené se subjektem údajů
   - poskytování služby, prodej zboží, zaslání výzvy ke splnění závazku
   - např. správce může zákonně zpracovávat jméno a adresu svého zákazníka, který si u něj objednal nějaké zboží, za účelem zaslání tohoto zboží na jeho adresu
3. Pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů

- Vždy je potřeba identifikovat základní účel daného závazku a osobní údaje následně pod tímto titulem zpracovávat pouze k jeho dosažení - účel nesmí být překročen

2. Plnění právní povinnosti správce

- Pouze pokud nějaký právní předpis členského státu či EU po správci požaduje, aby osobní údaje zpracovával, resp. aby prováděl určitou činnost, pro kterou je zpracování osobních údajů nezbytné
- Právní povinnost stanovena natolik určitě, aby z ní bylo možné poznat, jaká zpracování na jejím základě budou probíhat
- Musí to být právní povinnost - nikoliv pouze oprávnění
  - Správce nesmí mít na výběr, jestli povinnost splní, nebo ne
- Správce také nesmí mít nepřiměřenou možnost vlastního uvážení v tom, jak povinnost splní
- Správce nesmí překročit účel vyjádřený danou povinností

3. Ochrana životně důležitých zájmů

- Pouze v případech, kdy je osobní údaje nezbytné zpracovávat za účelem předejití vzniku újmy na životě subjektu údajů nebo jiné fyzické osoby
- K užití tohoto právního titulu by mělo být přistoupeno pouze, pokud není získání jiného titulu možné

Přijetí pacienta v bezvědomí do nemocnice, kdy nemocniční personál z tašky osoby zjistí její totožnost, aby mohl vyhledat údaje o této osobě v databázi nemocnice (např. ke zjištění alergií na léky atp.)

- Oproti současné právní úpravě odpadá nutnost dodatečného získání souhlasu s takovýmto zpracováním
- Po vyčerpání účelu zpracování není možné bez dalšího právního titulu údaje dále zpracovávat či uchovávat

4. Veřejný zájem či výkon veřejné moci

- Nový právní titul
- Pro zpracování osobních údajů orgány veřejné moci a soukromými subjekty, které jsou pověřeny výkonem určitého úkolu veřejné moci
- V případech, kdy **právní předpis dává správci určitý úkol ve veřejném zájmu a pro jeho splnění je nezbytné zpracovávat osobní údaje**
- Na rozdíl od plnění právní povinnosti není třeba výslovného příkazu ke zpracování a konkretizace zpracování v právním předpise
- Správce si může v rámci své zákonem stanovené diskrece zvolit, jakým způsobem úkol ve veřejném zájmu splní, a pokud při tomto způsobu bude potřeba zpracovávat osobní údaje, může je zpracovat na základě tohoto právního titulu
- Zpracování musí být nezbytné pro plnění daného úkolu + dodrženy všechny zásady zpracování

5. Oprávněný zájem

- Nejflexibilnější právní titul
- Správcem či zpracovatelem subjektivně stanovený zájem - zpravidla pro ochranu jeho vlastních práv či zájmů, kdy za účelem jeho dosažení je nezbytné zpracovávat osobní údaje
- Rozvaha, zda lze použít oprávněný zájem jako titul (balanční test):
  1. Jaký konkrétní zájem sleduji?
  2. Je zájem skutečně oprávněný a důležitý (váha)?
  3. Je zpracování pro daný zájem nezbytné?
  4. Jak moc zasáhnu do zájmů / základních práv a svobod subjektů údajů?
  5. Převáží oprávněný zájem (2.) nad zájmy/právy subjektů (3.)?
- Nutné informovat subjekt údajů o konkrétním oprávněném zájmu a o právu podat námitku (výslovně, odděleně a včas)

5. Oprávněný zájem
Příklady

- Ochrana majetku – např. při monitorování prostor kamerovým systémem

Vymáhání právních nároků

Předcházení škodám na počítačových systémech a systémech elektronických komunikací

Předávání správci v rámci skupiny podniků pro administrativní účely

Vědecký výzkum

Zpracování za účelem oznámení případných trestných činů

- Přímý marketing – zasílání obchodních sdělení stávajícím zákazníkům

Předcházení podvodům

Ochrana před zneužitím služeb

6. Souhlas subjektu údajů
Obecně

- Oproti nynějšku se souhlas jako titul posouvá z prvního místa na poslední
  - nejprve zkoumat, zda nenajdu jiný právní titul (oprávněný zájem?); pouze pokud nelze, využívat souhlas
- Správce musí být schopen doložit souhlas po celou dobu zpracování
- Souhlas rodičů v případě dětí mladších 16 let – dle nového návrhu zákona snížena hranice na 13 let věku dítěte

Bude možné použít současné souhlasy?

6. Souhlas subjektu údajů
Požadavky na souhlas

Svobodný

Skutečná možnost volby

Bez nátlaku a hrozby negativních důsledků v případě neudělení

Nesmí být nerovnováha mezi stranami

Členěný souhlas

Plnění smlouvy nesmí být závislé na souhlasu, když to pro plnění není nezbytné

Konkrétní

K určitému účelu zpracování

Subjekt údajů musí účel zpracování v době udělování souhlasu znát

Účel by měl být stanoven dostatečně specificky

Informovaný

Subjekt údajů informován o všech okolnostech zpracování v souladu s GDPR

Informace musí být sděleny ještě před udělením souhlasu

Jednoznačný

Prohlášení nebo jasné souhlasné jednání

- odlišitelné od ostatních informací
- ANO - aktivní zaškrtnutí políčka, podepsání listiny, výběr ve volbě ano/ne, zaslání e-mailu
- NE - implicitně, opt-out, předem zaškrtnuté políčko, zahrnutí souhlasu do VOP

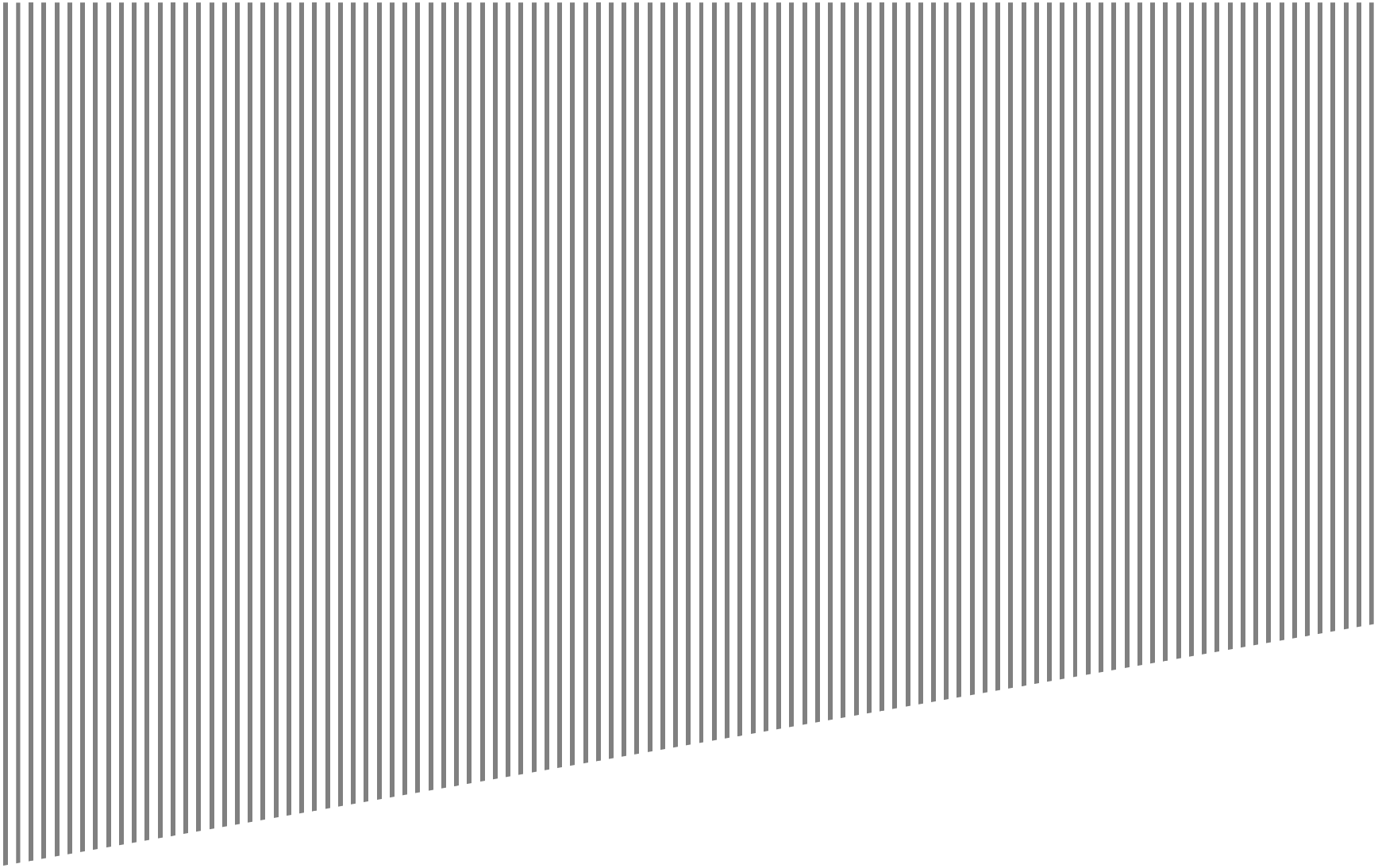
6. Souhlas subjektu údajů
Odvolání souhlasu

- Kdykoli odvolatelný
  - odvolání musí být stejně snadné, jako poskytnutí souhlasu
  - o právu na odvolání souhlasu nutno subjekt informovat
- Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním
- Důsledky pro správce
  - musí přestat osobní údaje zpracovávat pro určitý účel, ke kterému byl souhlas udělen
  - nemusí vždy znamenat povinnost osobní údaje zlikvidovat
  - správce může osobní údaje dále zpracovávat pro jiné účely, pro které využije jiný právní titul zpracování než souhlas

Kdy mohu zpracovávat „citlivé“ osobní údaje?

Výslovný souhlas	Ochrana životně důležitých zájmů
Údaje zjevně zveřejněné subjektem	Veřejný zájem v oblasti veřejného zdraví
Určení, výkon nebo obhajoba právních nároků a výkon soudních pravomocí	Významný veřejný zájem na základě unijního nebo vnitrostátního práva
Archivace, vědecký či historický výzkum a statistika	Zdravotní a sociální péče
Oprávněné činnosti neziskových subjektů sledujících politické, filozofické, náboženské nebo odborové cíle	Plnění povinností a výkon práv v oblasti sociálního zabezpečení a sociálního práva

3. Povinnosti správce



Základní povinnosti správce

„Papírové“ povinnosti

- **Širší informační povinnosti**
- Zpracování OÚ pouze ze zákonných důvodů – souhlas subjektu údajů a přísnější požadavky na něj
- **Zabezpečit soulad s GDPR** - dokumentovat zásady zpracování údajů, procesy a operace, a zpřístupnit je na žádost dozorujícímu úřadu – **záznamy o zpracování OÚ, kodexy, certifikace**

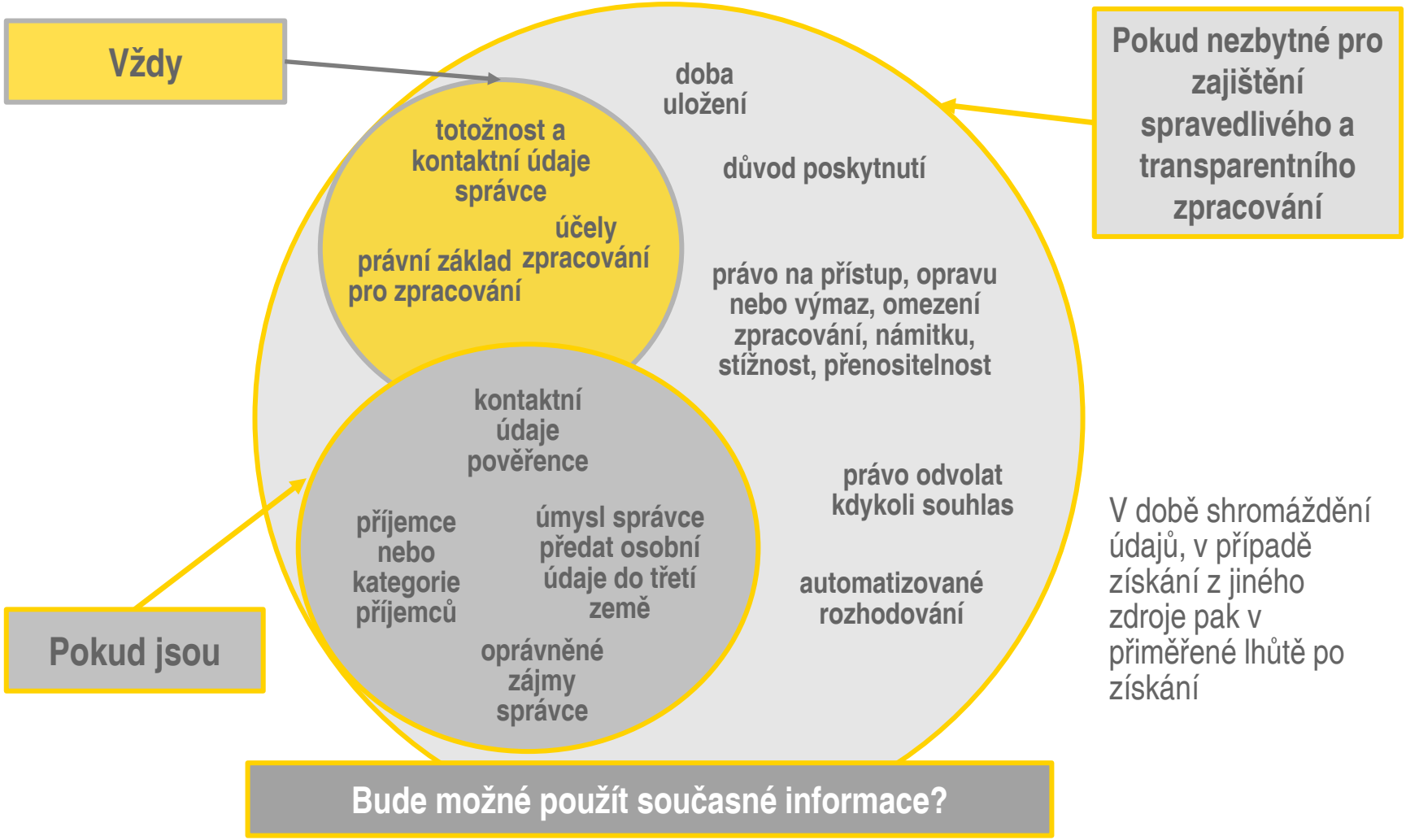
Procesní povinnosti

- Posouzení vlivu zpracování na ochranu OÚ před započetím zpracování **(analýza rizik)**
- Přijímání technických a organizačních opatření k ochraně údajů
- **Záměrná a standardní ochrana údajů**
- **Zabezpečení** údajů – pseudonymizace, šifrování atd.
- **Oznamování narušení zabezpečení** údajů
- Ustavení **pověřence** pro ochranu údajů

Způsob plnění povinností

- Stručným, transparentním, srozumitelným a snadno přístupným způsobem
- Písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě
- Za použití jasných a jednoduchých jazykových prostředků
  - vizualizace / standardizované ikony
  - otázky a odpovědi / vrstvené informace atp.
- Bezplatně
- Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce
  - uložit přiměřený poplatek zohledňující administrativní náklady, nebo
  - odmítnout žádosti vyhovět

Informační povinnost



Záznamy o činnostech zpracování

- Správce povinen vést záznamy o činnostech zpracování (interně)
  - zpřístupňuje je na žádost dozorovému úřadu
  - podobný rozsah informací, jako je v současné době správce povinen sdělovat ÚOOÚ v rámci oznamovací povinnosti – nahradí ji
  - výjimky: správci s méně než 250 zaměstnanci provádějící neriziková zpracování / nezpracovávající citlivé údaje
- Obsah:

Kontaktní údaje správce	Účel zpracování	Kategorie subjektů údajů	Kategorie osobních údajů
Kategorie příjemců údajů	Předávání do zahraničí	Lhůta pro výmaz	Technická a organizační opatření

Posouzení vlivu na ochranu osobních údajů („Privacy Impact Assessment“)

Co je PIA?	► Odpovědnost správce ► Nutné zejména při systematickém a rozsáhlém zpracování údajů a systematickém monitorování veřejně přístupných prostorů ► Možnost předchozí konzultace s ÚOOÚ před započetím se zpracováním osobních údajů
Jak PIA probíhá?	► Systematický popis zamýšleného zpracování ► Posouzení rizik z hlediska práv a svobod subjektů údajů ► Provedení testu proporcionality ► Plánovaná opatření ke zmírnění rizik
Kdy musím konzultovat s ÚOOÚ?	► Výsledek posouzení = zpracování je vysoce rizikové a riziko nelze zmírnit přiměřenými prostředky ► ÚOOÚ by měl následně zkoumat soulad zamýšleného zpracování s GDPR – pokud ne, doporučí správci úpravy zpracování

Posouzení vlivu na ochranu osobních údajů Příklady

Kamerový monitoring na pracovišti – pokud správce zamýšlí ukládat záznamy z kamer, dochází ke zpracování osobních údajů a správce musí posoudit vlivy uchovávání těchto údajů, jejich zabezpečení, možnost přístupu cizích osob atd.

Záměrná a standardní ochrana

„Privacy by design“ (záměrná ochrana)

- Správce/zpracovatel musí implementovat technická a organizační opatření k zajištění ochrany osobních údajů
- V praxi: vnitřní předpisy zaměstnavatele, opatření při zpracování osobních údajů kamerovými systémy

„Privacy by default“ (standardní ochrana)

- Nastavení systému zpracování pouze takových osobních údajů, jež jsou nezbytné pro dosažení specifikovaného účelu
- Minimalizace rozsahu zpracovávaných údajů
- Vymezení přístupových práv a subjektů oprávněných ke zpracování osobních údajů
- Doporučujeme revidovat osobní spisy zaměstnanců, zda rozsah zpracovávaných údajů odpovídá jejich účelu a je v souladu se zákonem

Zabezpečení údajů

- Každý správce musí přijmout adekvátní bezpečnostní opatření
  - odlišné s ohledem na rozsah, účel a povahu zpracování
- Krytá rizika
  - náhodné nebo protiprávní zničení, ztráta nebo pozměnění údajů
  - neoprávněné zpřístupnění údajů třetím osobám
  - neoprávněný přístup k údajům při přenosu, uložení nebo jiném zpracování
- Bezpečnostní opatření
  - šifrování, pseudonymizace
  - opatření pro zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování
  - proces pravidelného testování, posuzování a hodnocení účinnosti opatření

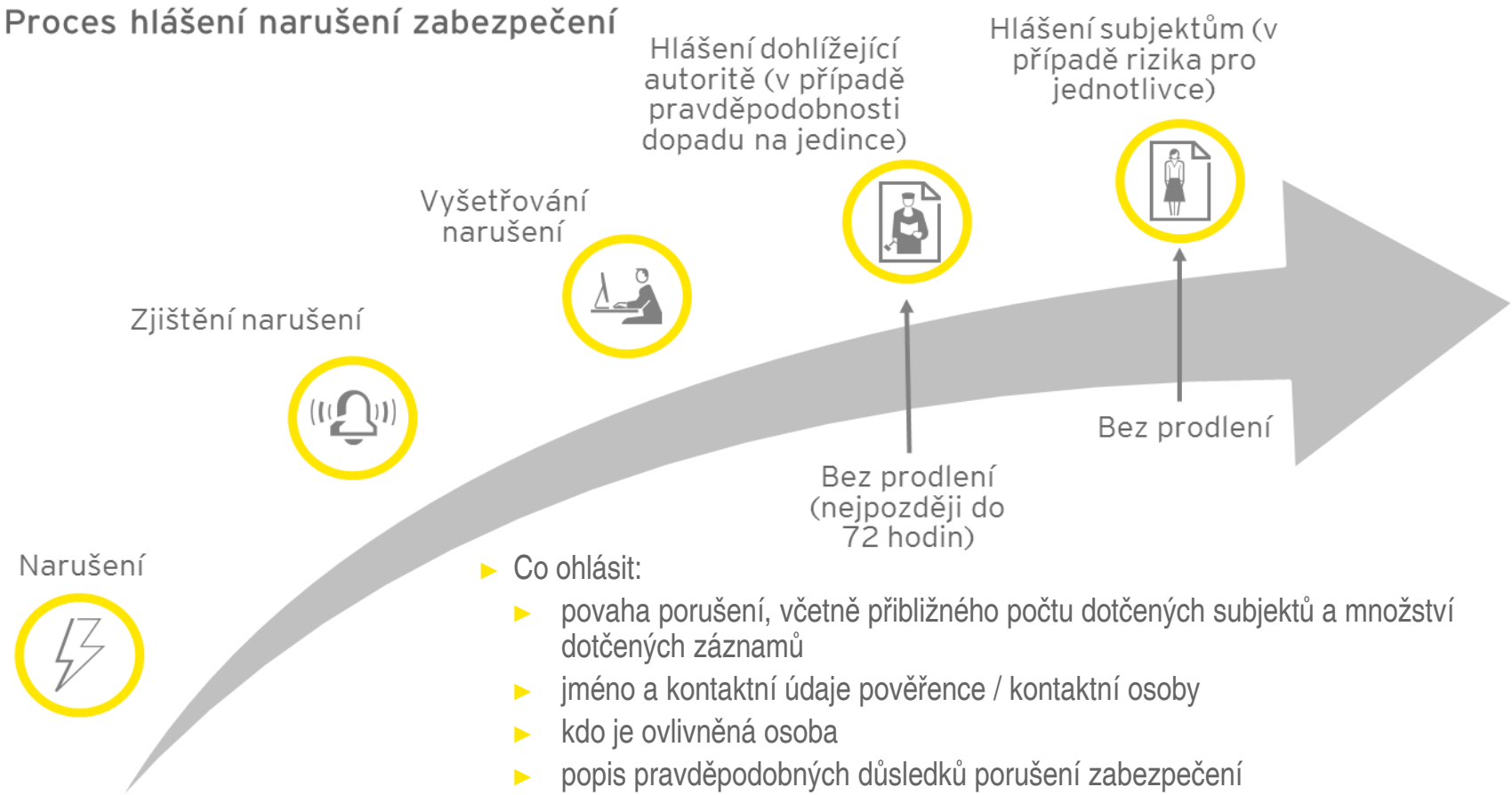
Pseudonymizace osobních údajů

- Osobní údaje nemohou být přiřazeny konkrétnímu subjektu údajů
- Jednoznačná identifikace subjektu údajů není možná bez „klíče“ (např. kód subjektu údajů přiřazený správcem)
- Bližší informace o subjektu údajů umožňující jeho identifikaci jsou uchovávány odděleně
  - správce přijme dostatečná opatření k jejich zabezpečení
- Dostatečný prostředek zajištění bezpečnosti osobních údajů, splňuje požadavky privacy by design

Pseudonymizace osobních údajů
Příklady

Osobní údaje zaměstnanců - tyto údaje jsou změněny pomocí klíče, zaměstnanci mají přiděleno osobní číslo (kód) a databáze jsou vedeny ve formě, ze které tyto údaje nelze přímo vyčíst. Klíč je uložen mimo tyto databáze a pomocí něj lze údaje uvést do původní podoby a přiřadit osobní údaje (identifikovat) zaměstnance

Oznamování narušení zabezpečení údajů



- Co ohlásit:
  - povaha porušení, včetně přibližného počtu dotčených subjektů a množství dotčených záznamů
  - jméno a kontaktní údaje pověřence / kontaktní osoby
  - kdo je ovlivněná osoba
  - popis pravděpodobných důsledků porušení zabezpečení
  - popis přijatých opatření správce s cílem vyřešit dané porušení
- Správci povinni vést **registr porušení a přijatých opatření**

4. Pověřenec pro ochranu osobních údajů

Kdo musí jmenovat pověřence?

- Správce i zpracovatel jsou povinni jmenovat vždy, kdy:
  - zpracování provádí orgán veřejné moci či veřejný subjekt (nikoli soudy jednající v rámci soudních pravomocí)
  - hlavní činnosti správce / zpracovatele spočívají v operacích zpracování vyžadujících rozsáhlé, pravidelné a systematické monitorování subjektů údajů (s ohledem na povahu, rozsah a účel operace)
  - hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování citlivých údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů
- I v jiných případech než výše uvedených, vyžaduje-li to národní legislativa – v návrhu zákona o zpracování osobních údajů není
- Vyhodnocení povinnosti jmenovat pověřence je na každém správci a zpracovateli - není-li zřejmé, zda vzniká povinnost jmenování, měla by být zpracována interní analýza

Co jsou „hlavní činnosti“ a „rozsáhlé zpracování“?

- Zásadní pojmy s ohledem na povinnost jmenovat pověřence
- Hlavní činnosti správce
  - souvisejí s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost
  - klíčové operace nezbytné k dosažení cílů správce / zpracovatele
  - např. hlavní činností nemocnice je poskytování zdravotní péče, která ji nemůže poskytovat bezpečně a účinně bez zpracování záznamů o pacientovi
- Rozsáhlé zpracování
  - dle množství zpracovávaných dat, počtu dotčených jednotlivců
  - např. zpracování zákaznických údajů v rámci běžné obchodní činnosti pojišťovny nebo banky
  - zpracování údajů (o obsahu, provozních, lokalizačních) poskytovatelem telefonních a internetových služeb

Jaká je role pověřence?

- Kontaktní bod a komunikace s dozorovým orgánem
- Posouzení rizik při zpracování osobních údajů
- Rady a doporučení správci/zpracovateli
- Dohled nad vedením záznamů o činnostech zpracování
- Zajištění souladu zpracování osobních údajů s GDPR
  - Pověřenec není odpovědný za nesoulad s požadavky ochrany osobních údajů
  - správce / zpracovatel musí vždy zajistit a doložit, že zpracování osobních údajů probíhá v souladu s GDPR
- Je vázán mlčenlivostí – i po skončení výkonu činnosti pověřence

Forma spolupráce s pověřencem

- Musí být reálně dostupný (doporučení, aby pověřenec sídlil v EU bez ohledu na sídlo správce / zpracovatele)
- Může být jeden v rámci skupiny společností, pokud bude snadno dosažitelný z každé z nich (s přihlédnutím ke struktuře a velikosti organizace)

A. Zaměstnanec správce / zpracovatele
   - odpovídá dle zákoníku práce
   - omezené důvody výpovědi – nesmí být propuštěn či sankcionován v souvislosti s plněním svých úkolů (i pro externího pověřence)

A. Spolupráce na externí bázi
   - smlouva o poskytování služeb
   - musí rovněž splňovat podmínky nařízení
   - ve smlouvě by měly být uvedeny jednotlivé úkoly pověřence

Odborné požadavky na osobu pověřence

- Musí být jmenován na základě svých **profesních kvalit** - odborné znalosti práva a praxe v oblasti ochrany údajů a schopnost plnit úkoly stanovené v GDPR
- Úroveň odborných znalostí - dle prováděných operací zpracování a podle ochrany požadované pro zpracovávané OÚ – úměrnost k citlivosti, složitosti a množství zpracovávaných dat
- Profesní kvality – znalost národní a evropské legislativy, praxe v oboru ochrany OÚ, znalost chodu a oboru podnikání správce / zpracovatele, znalost prováděných operací zpracování, IS, bezpečnosti dat
- Nemusí mít právnické vzdělání

Povinnosti správce / zpracovatele vůči pověřenci

- Správce / zpracovatel pověřenci zajistí:
  - poskytnutí zdroje k plnění úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí
  - aktivní podporu od vyššího managementu
  - dostatečný čas pro plnění povinností (zejména u částečného úvazku)
  - odpovídající finanční podporu
  - dostatečnou infrastrukturu (vybavení, prostory, zařízení)
  - odpovídající personál (v závislosti na velikosti a struktuře správce / zpracovatele může vyvstat potřeba sestavení týmu)
  - oficiální oznámení o jmenování pověřence všem zaměstnancům
  - nezbytný přístup do jiných oddělení (personální, IT, právní, atd.)
  - průběžné školení pověřence (zvyšování úrovně znalostí)
  - nedávání pokynů týkající se výkonu úkolů pověřence

Úkoly pověřence
Interní

- Poskytuje informace a poradenství správcům / zpracovatelům a jejich zaměstnancům, kteří provádějí zpracování osobních údajů
- Kontroluje zpracování osobních údajů v rámci společnosti
- Implementuje GDPR a monitoruje soulad s ním a jinými právními předpisy
- Tyto úkoly zahrnují zejména:
  - vývoj a pravidelnou aktualizaci programů na ochranu OÚ
  - vzdělávání dalších zaměstnanců společnosti, kteří se podílí na zpracování OÚ
  - informování vedení společnosti o strategiích a rizicích
  - sledování právního a politického vývoje v oblasti ochrany OÚ
  - vypracování zásad ochrany osobních a firemních údajů

Úkoly pověřence
Posouzení vlivu

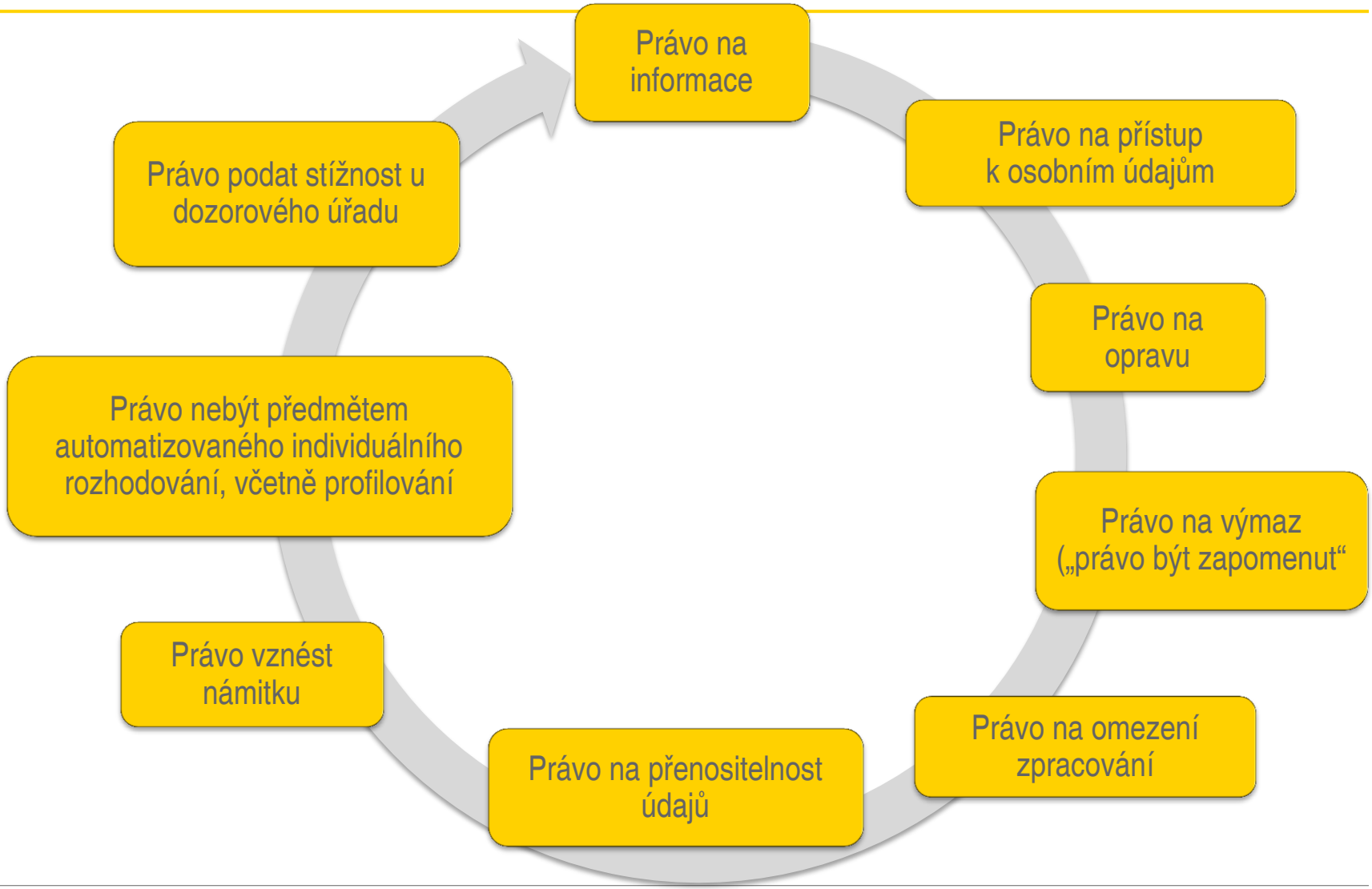
- Poskytuje poradenství na požádání k posouzení vlivu na ochranu osobních údajů
  - správce je povinen si vyžádat posudek pověřence při provádění posouzení vlivu
  - k této povinnosti pracovní skupina vydala doporučení, aby si správce vyžádal posudek k těmto otázkám:
    - nutnost provedení posouzení vlivu
    - jakou metodiku použít
    - jaká ochranná opatření uplatnit pro zmírnění rizik pro zájmy a právy subjektů
    - zda jsou závěry v souladu s nařízením
    - nesouhlasí-li správce s posudkem, měl by zdokumentovat důvody

Úkoly pověřence
Externí

- Spolupracuje s dozorovým úřadem
  - jedná jako kontaktní osoba ohledně zpracování osobních údajů
  - usnadňuje dozorovému úřadu přístup k dokumentům a informacím pro výkon úkolů dozorového úřadu, i pro uplatňování jeho vyšetřovacích, nápravných, povolovacích a poradních pravomocí
  - Může požádat dozorový úřad o radu, popř. vést s ním konzultace v jakékoli věci ve vztahu k osobním údajům
- Je kontaktní osobou i pro subjekty údajů (uvnitř i mimo organizaci)

5. Posílení práv subjektů údajů

Přehled práv subjektů údajů



Právo na přístup k osobním údajům

- Na žádost subjektu údajů správce sdělí, zda zpracovává osobní údaje žadatele a případné další informace:
  - účely zpracování
  - kategorie dotčených osobních údajů – všechny údaje, které se týkají žadatele (nejen ty, které sám poskytl)
  - příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny
  - plánovaná doba, po kterou budou osobní údaje uloženy (příp. kritéria použitá k jejímu určení)
  - práva subjektu údajů vztahující se ke zpracování osobních údajů, které se ho týkají – právo na opravu, právo na výmaz atd.
- Správce reaguje na žádost ve lhůtě jednoho měsíce s možností jejího prodloužení o další dva měsíce

Právo na přístup k osobním údajům
Příklady

Uchazeč o zaměstnání, který zaslal společnosti životopis / zaměstnanec / zákazník společnosti požádá společnost o sdělení, zda zpracovává jeho osobní údaje

Právo na opravu údajů

- Na žádost subjektu údajů ověření, zda jsou osobní údaje správné, přesné atd.
- Do doby ověření je zpracování omezeno
- Osobní údaje jsou správné a přesné - správce subjekt údajů informuje, že omezení bude zrušeno a že bude ve zpracování osobních údajů pokračovat
- Osobní údaje nejsou správné a přesné - správce poskytne informace o přijatých opatřeních
- Správce by měl zajistit podmínky pro to, aby žádosti na opravu mohly být podávány online, zejména v případě zpracování OÚ elektronickými prostředky

Právo být zapomenut

- Rozšířené právo na výmaz osobních údajů, zejména pokud
  - osobní údaje nejsou již potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
  - subjekt údajů odvolal svůj souhlas se zpracováním,
  - subjekt údajů vznesl námitku proti zpracování osobních údajů,
  - osobní údaje jsou zpracovávány protiprávně atd.
- Smyslem je zamezit řetězení osobních údajů a šíření nepravdivých či škodlivých údajů (např. v internetových vyhledávačích, sociálních sítích)
- Výjimky: může být omezeno právem na svobodný přístup k informacím či dalšími právem chráněnými zájmy (ochrana veřejného zdraví, archivnictví, statistické účely, výzkum) – nutnost nastavení vhodných záruk pro ochranu práv a svobod subjektu údajů

Právo být zapomenut
Příklady

Správce má povinnost na žádost subjektu údajů (např. zákazníka / uchazeče o zaměstnání) odstranit veškeré osobní údaje, a to bez zbytečného odkladu

Správce rovněž odpovídá za odstranění osobních údajů zákazníků, které shromažďují zpracovatelé (např. dopravci společnosti rozvážející výrobky zákazníkům společnosti).

Právo na omezení zpracování

- Podobné dnešnímu právu blokace, které je slabším právem
- Subjekt údajů má právo na omezení zpracování v těchto případech:
  - subjekt údajů popírá přesnost – na dobu ověření přesnosti
  - zpracování je protiprávní a subjekt údajů odmítá výmaz údajů a místo toho žádá o omezení jejich použití
  - správce již údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků
  - subjekt údajů vznesl námitku - dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů
- Správce posoudí žádost bez zbytečného odkladu od obdržení žádosti - nejpozději do jednoho měsíce buď provede omezení zpracování nebo odmítne výkon práva nebo prodlouží lhůtu
- Správce musí informovat o výsledku posouzení a o přijatých opatřeních

Právo na přenositelnost údajů I.

- Subjekt údajů může požádat, aby údaje předal jeden správce správci druhému – informační povinnost správce
- Cílem je usnadnit přesun, kopírování a předávání osobních údajů z jednoho IT prostředí do jiného
- Podpora soupeření mezi správci, kterými budou zejména poskytovatelé internetových služeb a e-commerce - zvýšení kvality poskytovaných služeb
- Měly by být omezeny situace, kdy subjekt údajů zůstává u používání jedné služby a nezačne používat jinou jen z toho důvodu, že již investoval velké množství času do využívání první
- Právem obdržet osobní údaje nejsou dotčena právo být zapomenut ani právo námitky proti zpracování
- Uplatnění práva neznamená výmaz osobních údajů

Právo na přenositelnost údajů II.

- Za splnění dvou podmínek:
  - zpracování osobních údajů je založeno na souhlasu nebo na smlouvě a
  - zpracování je prováděno automatizovaně
- Posiluje kontrolu subjektu údajů nad svými údaji
- Strukturovaný, běžně používaný a strojově čitelný formát
- Podmínkou je technická proveditelnost

Právo na přenositelnost údajů
Příklady

Zaměstnanecká data - v praxi se právo na přenositelnost v oblasti personalistiky bude týkat např. výplat a náhrad, vnitřního náboru zaměstnanců, avšak v mnoha jiných situacích bude potřeba případ od případu ověřit, zda jsou splněny všechny podmínky týkající se práva na přenositelnost údajů – zda jsou OÚ zpracovávány na základě souhlasu zaměstnance (a nejedná se o plnění zákonných povinností), zda jsou zpracovávány automatizovaně (ne papírové osobní spisy).

Právo vznést námitku

- Týká se případů zpracování z titulu oprávněného zájmu nebo veřejného zájmu
- Správce musí osobní údaje subjektu údajů, který vznesl námitku, bez zbytečného odkladu přestat zpracovávat
- Zpracování může pokračovat, pouze pokud správce prokáže závažné oprávněné důvody
  - pro zpracování, které převažují nad právy subjektu údajů
  - pro určení, výkon nebo obhajobu právních nároků
- Oprávněný zájem = přímý marketing
  - údaje již nebudou pro tyto účely zpracovávány – bez dalšího zkoumání
- Subjekt údajů musí být na toto právo výslovně upozorněn a toto právo by mělo být uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději při první komunikaci se subjektem údajů

.

Právo vznést námitku
Příklad

Registrace uchazečů o zaměstnání do databáze společnosti – společnost musí upozornit zaměstnance na právo vznést námitku proti zpracování jejich osobních údajů

Zpracování -> námitka subjektu údajů (např. zákazníka) ->

(i) správce dále nezpracovává, nebo

(ii) prokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy/právy a svobodami zákazníka.

Právo nebýt předmětem automatizovaného individuálního rozhodování

- Zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování (včetně profilování)
- O právech či povinnostech subjektu údajů (nebo o podobně závažných skutečnostech, které na něj mají dopad) rozhoduje výlučně algoritmus (předem stanovený postup, který je následně prováděn automatizovaně)
- Automatizované rozhodnutí je přípustné, pokud
  - je nezbytné k uzavření smlouvy mezi subjektem údajů a správcem
  - je povoleno právem EU nebo členským státem
  - je založeno na výslovném souhlasu subjektu údajů

Právo nebýt předmětem automatizovaného individuálního rozhodování - příklady

Nábor nových zaměstnanců - společnost zavede algoritmus, který profiluje uchazeče o zaměstnání, zda je vhodný pro danou práci a na základě tohoto profilování je rozhodnuto, zda s ním zaměstnavatel uzavře pracovní smlouvu

Zaměstnavatel na základě výhradně automatizovaného rozhodnutí vyvodí pro zaměstnance pracovněprávní důsledky, např. ukončení pracovního poměru, nepřiznání bonusu atp.

Právo podat stížnost u dozorového úřadu

6. Předávání osobních údajů

Předávání osobních údajů obecně

- Správce může přibrat jiný subjekt, který pro něj OÚ zpracovává
  - nutné dostatečné záruky zpracovatele ohledně vhodných technických a organizačních opatření s ohledem na povahu, kontext, kategorii údajů
  - zákonné zmocnění nebo smlouva o zpracování osobních údajů
  - zpracování prostřednictvím zpracovatele musí splňovat požadavky GDPR a musí zajistit ochranu práv subjektů údajů
  - správce se přizváním zpracovatele nezbavuje odpovědnosti za zpracování osobních údajů

X

- Předání údajů jinému správci => nutné mít právní titul pro zpracování

Předání osobních údajů zpracovateli
Příklad

Předání osobních údajů externí mzdové účtárně

Nutná smlouva o zpracování osobních údajů

Předávat pouze nezbytné údaje

Povinnost informovat zaměstnance

Smlouva o zpracování osobních údajů

- Smlouva musí být uzavřena vždy, když **pro správce** zpracovává osobní údaje někdo jiný bez zákonného zmocnění
- Písemná forma (včetně elektronické)
- Nemusí se jednat o samostatnou smlouvu
- Obsah:

Předmět a doba trvání zpracování	Povaha a účel zpracování	Typ osobních údajů a kategorie subjektů údajů	Vázanost doloženými pokyny správce	Mlčenlivost
Zabezpečení	Řetězení zpracovatelů	Součinnost	Umožnění inspekcí a auditů	Ukončení zpracování

Povinnosti a odpovědnost zpracovatele

- V podřízeném postavení vůči správci – údaje zpracovává pouze k účelu, pro který mu byly svěřeny a v souladu s pokyny správce
  - pokud poruší GDPR tím, že určí nový účel zpracování => považuje se ve vztahu k tomuto zpracování za správce => odpovědnost a povinnosti
- Vede záznamy o zpracování
- Spolupracuje s dozorovým úřadem
- Zavádí vhodná technická a organizační opatření k zajištění odpovídající úrovně zabezpečení
- Hlásí případná porušení zabezpečení osobních údajů správci
- Odpovídá za újmu způsobenou zpracováním pouze v případě, že nesplnil povinnosti stanovené mu GDPR, nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi

Řetězení zpracovatelů

- Není a priori zakázáno
- Správce, který primárně odpovídá za zpracování osobních údajů, by měl vědět, které subjekty pro něj osobní údaje zpracovávají
- Možné jen s písemným povolením správce
  - ke konkrétnímu dalšímu zpracovateli
  - obecné svolení => zpracovatel musí správce informovat o veškerých přijetích dalších zpracovatelů nebo jejich nahrazení
- Nutné závazně přenést na dalšího zpracovatele stejné povinnosti, jaké ukládá smlouva o zpracování zpracovateli
- Porušení povinností dalšího zpracovatele => správci odpovídá první zpracovatel

Předávání osobních údajů do třetích zemí

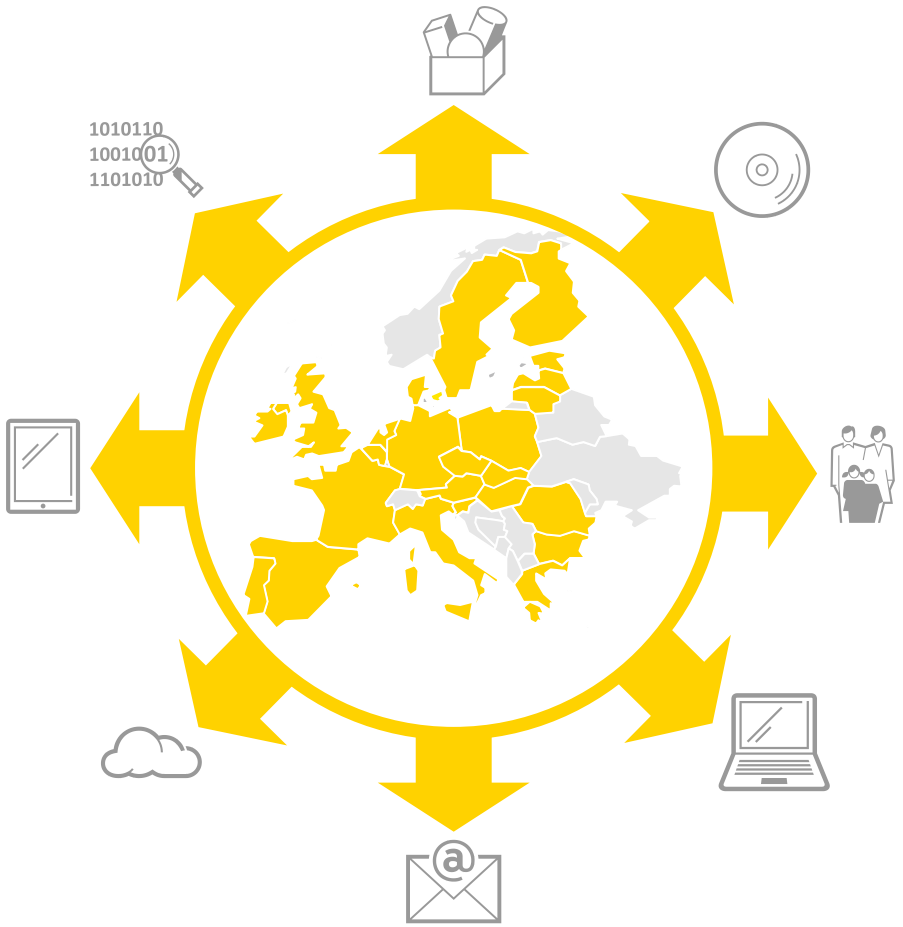
- V rámci ČR/EU(EHP) volný pohyb osobních údajů
- Pro předávání údajů do třetích zemí nutné splnit zvláštní podmínky
  - mezinárodní smlouva nebo podmínky dle GDPR
- Předávání os. údajů do zahraničí = jakékoliv sdělení, zpřístupnění nebo jiné poskytnutí osobních údajů správci či zpracovateli ve třetí zemi mimo EU
- O předání do třetí země se nejedná, pokud jsou osobní údaje zveřejněny na internetu a má k nim přístup kdokoliv odkudkoliv na světě

Předávání osobních údajů do třetích zemí

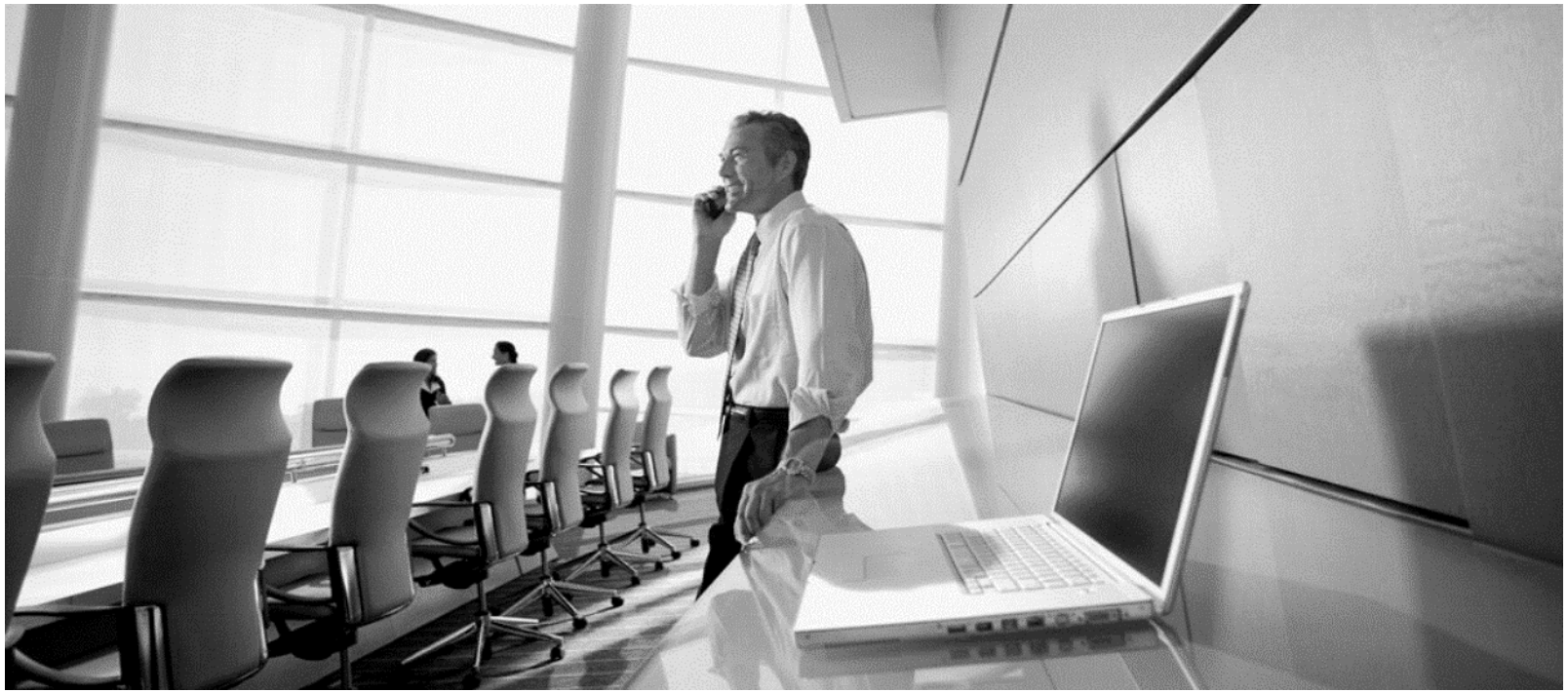
GDPR povoluje předávání osobních údajů do třetích zemí za předpokladu **zajištění odpovídající úrovně ochrany údajů:**

- rozhodnutí EK o odpovídající ochraně pro danou zemi
- standardní doložky o ochraně údajů
- závazná podniková pravidla (BCRs)
- schválený kodex chování nebo certifikační mechanismus (například „European Data Protection Seal“)

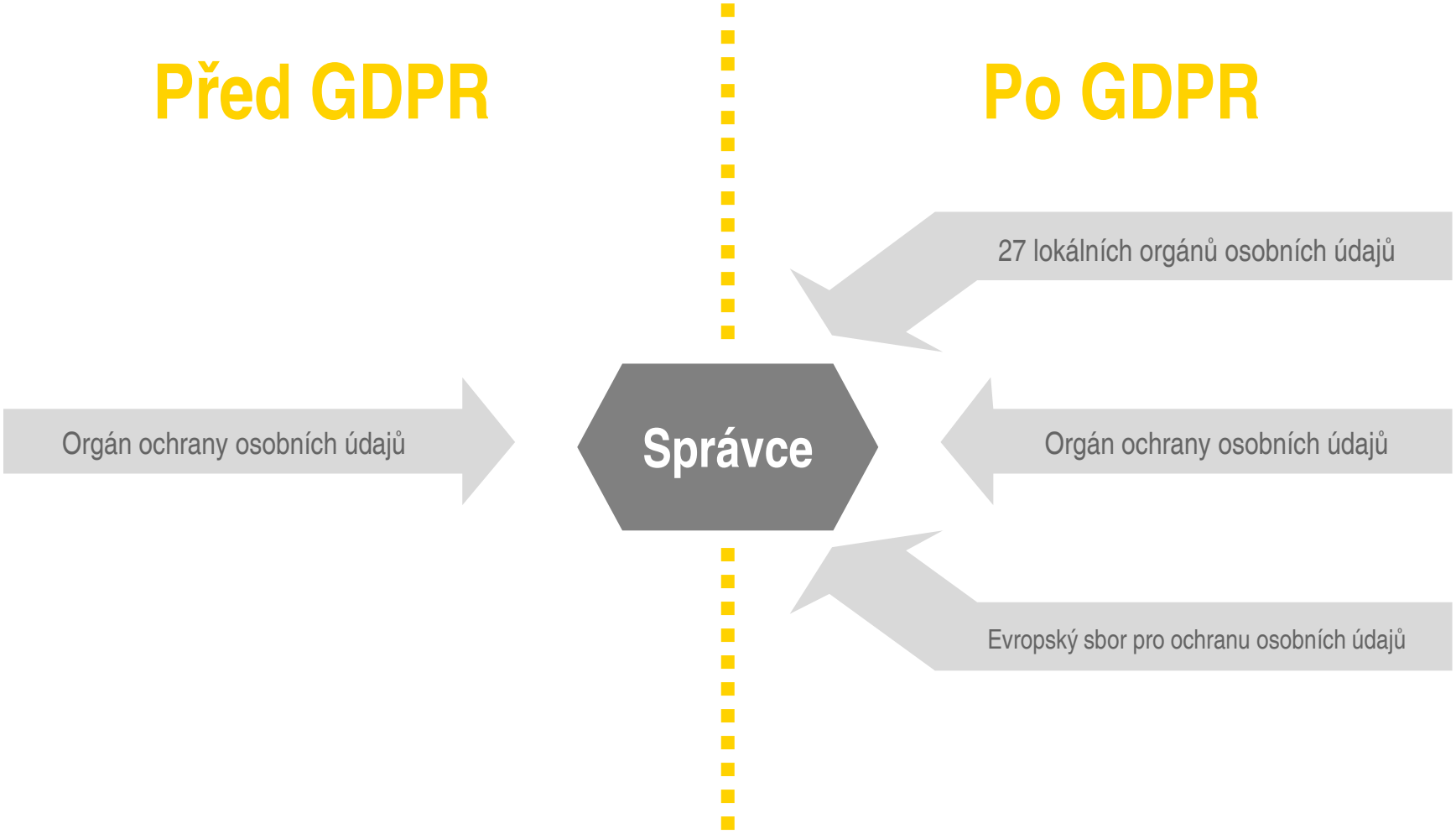
Již nebude nutné předchozí povolení ÚOOÚ



7. Orgány ochrany osobních údajů



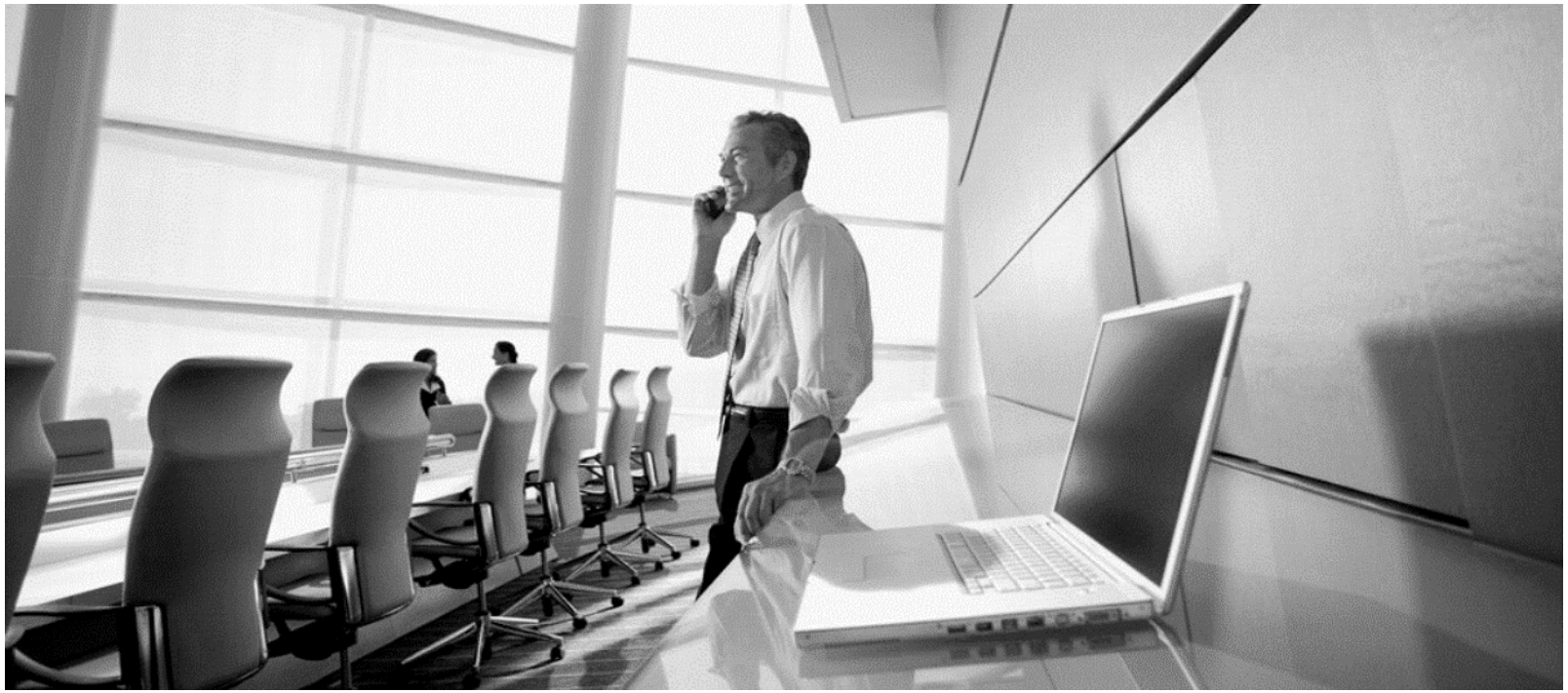
Orgány ochrany osobních údajů I.



Orgány ochrany osobních údajů II.

- Vedoucí dozorový úřad jako one-stop shop
  - v ČR zůstává ÚOOÚ
- Evropský sbor pro ochranu osobních údajů (nynější Pracovní skupina)
  - nejvyšší dozorový orgán
  - dozor nad zajištěním jednotné aplikace GDPR po celé EU
  - tvořen vedoucími dozorových úřadů z každého členského státu a evropským inspektorem ochrany údajů

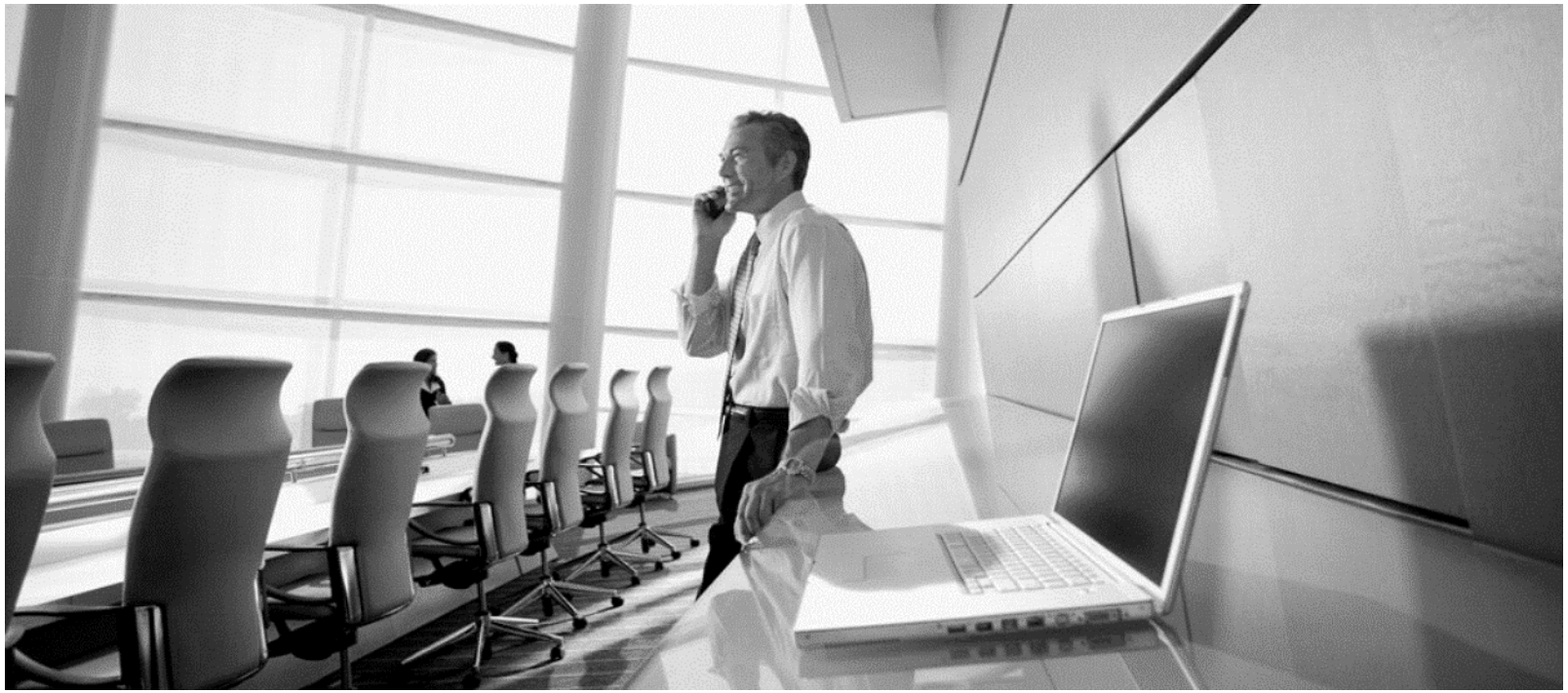
8. Sankce



Sankce

- Při porušení základních zásad zpracování osobních údajů
- Primárně odstrašující charakter sankcí
- Až do výše **4 % ročního celosvětového obratu podniku nebo 20 milionů EUR** (podle toho, co je vyšší)
- Lze očekávat tlak na sjednocení výše pokut v rámci EU

9. Jak se nachystat na GDPR?



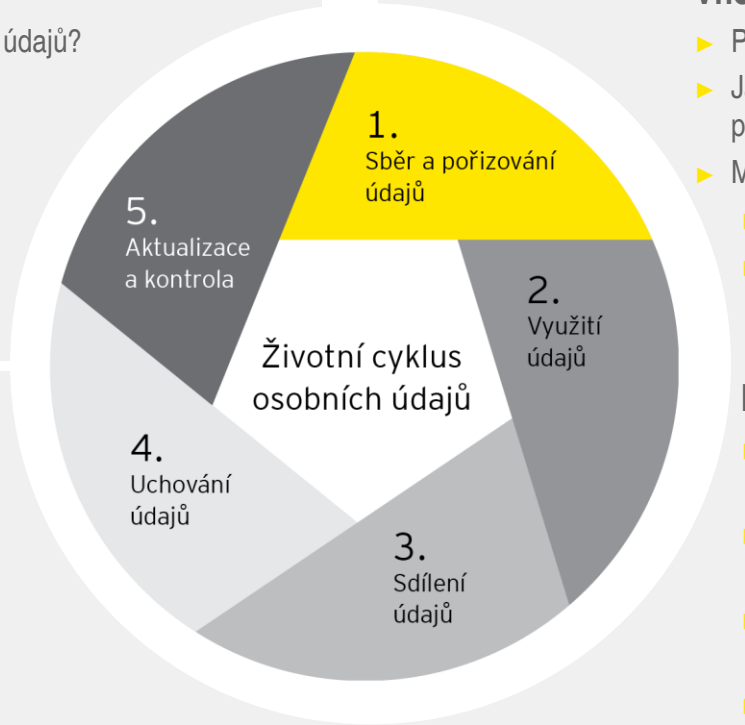
Životní cyklus osobních údajů

Přiměřené uchování údajů

- Definovány lhůty pro uchování údajů?
- Nepotřebné údaje mazány, anonymizovány?
- Údaje řádně zabezpečeny?
- Provedeno šifrování/ pseudonymizace?

Oprávněné sdílení

- Data předávána příjemcům?
- Uzavřena smlouva o zpracování?
- Data přenášena mimo ČR/EU?
- Vhodné záruky?



Vhodné pořizování údajů

- Posouzení vlivu zpracování
- Jaké kategorie údajů jsou pořizovány?
- Mám právní titul a legitimní účel?
  - Je třeba souhlas subjektu?
  - Je subjekt informován o zpracování?

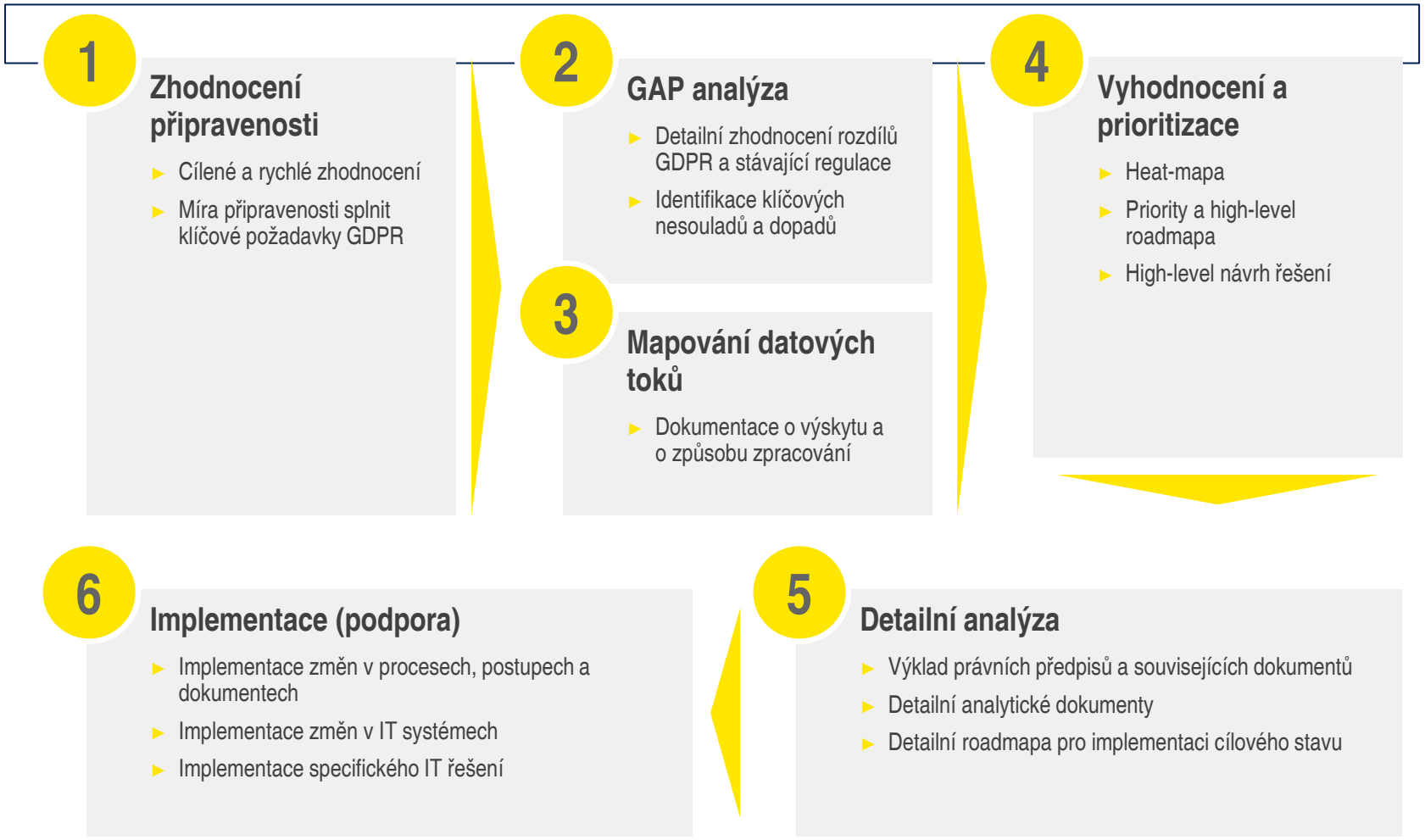
Relevantní využití údajů

- K jakému účelu jsou údaje využívány?
- Jakým způsobem jsou údaje využívány?
- Využity pro automatizované rozhodování?
- Záznamy o zpracování

Klíčové právní otázky zpracování osobních údajů

Checklist - audit zpracování osobních údajů	
	Ověřit/upravit právní tituly pro zpracování údajů
	Prověřit použitelnost udělených souhlasů
	Vypracovat a předat nové informace o zpracování údajů
	Zavést záznamy o činnostech zpracování
	Zkontrolovat technická a organizační opatření k ochraně údajů
	Předávány údaje? Splněny všechny související povinnosti? Revize smluv se zpracovateli
	Nutno jmenovat pověřence?
	Nutno provést posouzení vlivu? Pokud ne – zdokumentovat

Rozfázování GDPR projektu



Weinhold Legal

Diskuse

Kontaktní údaje

Mgr. Tomáš Čermák, advokát
Tomas.Cermak@weinholdlegal.com

Mgr. Nikola Faltová, advokátní koncipientka
Nikola.Faltova@weinholdlegal.com

Tento seminář pořádá
Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz

Děkujeme za Vaši pozornost!