PŘÍPRAVA NA GDPR – METODIKA HL. M. PRAHY

1. ÚVOD

Účelem této metodiky hl. m. Prahy je přehledně shrnout kroky, které musí provést hl. m. Praha, její městské části a jimi zřizované příspěvkové organizace k tomu, aby řádně vyhověly požadavkům nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**"). Tato metodika si klade za cíl usnadnit postup osobám zajišťujícím soulad s GDPR a pomoci jim co možná chránit své organizace před sankcemi, které v budoucnu mohou být uloženy dozorovými orgány a které mohou být velmi citelné.

Tento dokument nemůže nahradit expertní stanovisko k specifickým dopadům GDPR na danou organizaci či na některé z jejích agend, nicméně měl by v dostatečném rozsahu umožnit čtenáři základní porozumění aktuálních otázek spojených s nakládáním s osobními údaji.

1.1 CO JE GDPR

GDPR je nařízení EU, které bude účinné od 25. května 2018 a které se bude přímo aplikovat ve všech členských zemích včetně České republiky. Do uvedeného data (25. května 2018) se budou muset všechny složky hl. m. Prahy a její městské části – coby správci osobních údajů (a případně též jejich zpracovatelé, viz níže bod 2.) připravit na nová pravidla, nastavit procesy a upravit související dokumentaci, tak aby se vyhnuly riziku potenciálních mnohonásobně vyšších pokut a dalším následkům spojeným s nesprávným zacházením s osobními údaji. Nařízení EU nahrazuje v tomto směru dosud platný český zákon č. 101/2000 Sb., o ochraně osobních údajů, přičemž pokuty a následky zaváděné nařízením GDPR jsou výrazně přísnější.

Vzhledem k tomu, že se u GDPR jedná o evropské *nařízení* (nejde tedy o směrnici), bude GDPR použitelné přímo a jednotně ve všech státech EU. Práva a povinnosti vyplývají přímo z textu nařízení GDPR. GDPR je dostupné v českém jazyce a od své účinnosti nahradí dosavadní českou národní úpravu v této oblasti. Český Úřad pro ochranu osobních údajů však bude nadále existovat a působit jako dozorový a kontrolní orgán v oblasti osobních údajů.

1.2 JAKÉ HLAVNÍ ZMĚNY PŘINÁŠÍ OPROTI DNEŠNÍMU STAVU

- **Nové a širší pojmy** (čl. 4 GDPR): rozšíření stávajících definic (osobní údaj, zvláštní kategorie osobních údajů) a nové pojmy (omezení zpracování, pseudonymizace, profilování, porušení zabezpečení osobních údajů, pověřenec pro ochranu osobních údajů atd.)
- **Univerzální územní působnost** (čl. 3 GDPR): efektivní postihování i správců, kteří nemají sídlo v EU
- **Souhlas se zpracováním osobních údajů**: rozšíření definice souhlasu se zpracováním osobních údajů (čl. 4 odst. 11 GDPR), zpřísnění podmínek pro získání souhlasu (čl. 7 GDPR) a stanovení pravidel týkajících se nezletilých (čl. 8 GDPR)
- **Rozšíření práv subjektů údajů** (čl. 12-23 GDPR): více práv pro jednotlivce (přenositelnost osobních údajů, právo být zapomenut, právo na první bezplatnou kopii osobních údajů, právo vznést námitku, právo na omezení zpracování osobních údajů)
- **Detailnější důraz na zajištění bezpečnosti** (čl. 32 GDPR):
  - zavedení vhodných technických a organizačních opatření (např. pseudonymizace a šifrování osobních údajů);
  - schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
  - schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů;

- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování

- **Ohlašování incidentů** (čl. 33 GDPR): povinnost ohlašovat Úřadu pro ochranu osobních údajů případy porušení zabezpečení osobních údajů bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy se o něm správce dozvěděl [až na výjimky nutno oznámit i subjektům údajů (čl. 34 GDPR)]
- **Záznamy o činnostech zpracování** (čl. 30 GDPR): formální oznámení o zpracování osobních údajů Úřadu pro ochranu osobních údajů (tzv. registrace) bude nahrazeno detailnější povinností vést interní záznamy o zpracování osobních údajů
- **Posouzení vlivu na ochranu osobních údajů a předchozí konzultace** (čl. 35 a 36 GDPR): je-li pravděpodobné, že určité zpracování, zejména při využití nových technologií, bude z pohledu Úřadu pro ochranu osobních údajů rizikové, povinnost vypracovat dopady na ochranu osobních údajů a v některých případech je konzultovat s Úřadem (ten sestaví a zveřejní seznam zpracování podléhajících tomuto požadavku)
- **Pověřenec ochrany osobních údajů** (čl. 37 GDPR): povinnost v některých případech jmenovat uvnitř organizace „pověřence pro ochranu osobních údajů", nebo takovou osobu zajistit externě (zejm. u rozsáhlého a systematického monitorování subjektů údajů)
- **Významné pokuty připomínající sankce na úseku hospodářské soutěže** (čl. 83 odst. 6 GDPR): porušení pravidel ochrany osobních údajů může být pokutováno částkou až 20 mil. EUR, anebo 4 % celosvětového obratu, podle toho, co je vyšší (novým zákonem navazujícím na GDPR bude pro orgány veřejné moci pravděpodobně zaveden strop výše pokuty)

2. KDO A S JAKÝMI OSOBNÍMI ÚDAJI NAKLÁDÁ NA MUNICIPÁLNÍ ÚROVNI

Na úrovni hl. m. Prahy s osobními údaji nakládají jednak manuálně její zaměstnanci, příspěvkové organizace či obchodní partneři, a jednak dochází k automatizovanému zpracování osobních údajů prostřednictvím počítačových programů, které hl. m. Praha používá.

Hl. m. Praha, její městské části a jimi zřizované příspěvkové nebo jiné organizace mohou vystupovat současně ve více rolích, s čímž jsou spojeny různé povinnosti. První rolí je ***správce*** osobních údajů (čl. 4 odst. 7 GDPR); správce je povinen stanovit účel a prostředky zpracování osobních údajů a zajistit jejich náležité zabezpečení. Druhou rolí je ***zpracovatel*** osobních údajů (čl. 4 odst. 8 GDPR8), který smí zpracovávat osobní údaje pouze dle pokynů správce; přesto i na zpracovatele mohou dopadnout sankce (fakultativně spoluodpovídá za porušení povinnosti správce a povinně asistuje správci při reagování na uplatnění práv subjektů údajů).

Níže jsou uvedeny typické oblasti, které je třeba posoudit pro určení, zda jsou hl. m. Praha, její městské části a jimi zřizované příspěvkové nebo jiné organizace připraveni na GDPR.

2.1 VEŘEJNÁ SPRÁVA

2.1.1 Přenesená působnost

Na úseku přenesené působnosti dochází ke zpracování osobních údajů zejména v následujících oblastech (s uvedením typických příkladů zpracovávaných osobních údajů):

- sociálně-právní ochrana dětí
  především půjde o údaje stanovené zákonem o sociálně-právní ochraně dětí, např. osobní údaje dětí, jejich rodičů, údaje o výchovných poměrech těchto dětí, záznamy o výsledcích šetření v rodině, záznamy o jednání s rodiči nebo jinými osobami, kopie podání soudům a jiným státním orgánům, písemná vyhotovení rozhodnutí soudů, atd.; součástí spisové dokumentace mohou být také zvukové, obrazové a zvukově obrazové záznamy na elektronických médiích; dále může být vedena evidence pro zprostředkování osvojení a pěstounské péče

- evidence obyvatel
  v zásadě půjde o všechny osobní údaje stanovené zákonem o evidenci obyvatel
- občanské průkazy a cestovní doklady
  půjde o údaje uvedené v zákoně o občanských průkazech a v zákoně o cestovních dokladech, a to v souvislosti s vyřizováním žádostí o vydání občanských průkazů anebo cestovních dokladů obsahujících řadu osobních údajů, příp. se může jednat také o biometrické údaje v rámci kontroly funkčnosti nosičů dat s biometrickými údaji
- hazardní hry
  především se jedná o údaje v souvislosti s povolováním hazardních her např. jméno a příjmení žadatele – fyzické osoby – získané v rámci povolovacího řízení a poskytování informací ministerstvu, dále např. údaje o osobě, která bude zajišťovat řádný průběh hazardní hry (tombola a turnaje malého rozsahu) a dodržování podmínek stanovených zákonem o hazardních hrách
- živnostenské podnikání
  např. přidělení identifikačního čísla osoby či zápis nové adresy její provozovny, a další údaje v souvislosti s provozováním živnostenského rejstříku
- řízení o některých přestupcích
  např. osobní údaje všech účastníků přestupkového řízení, videozáznamy či fotografie osob
- rozhodování o poskytování opakujících se peněžitých dávek
  např. osobní údaje z evidence uchazečů/zájemců o zaměstnání, údaje o výši poskytnutých dávek
- státní občanství
  zejm. využívání údajů z registru obyvatel, informačních systémů evidence občanských průkazů, cestovních dokladů, diplomatických a služebních pasů, z informačního systému cizinců
- matriční knihy
  týká se vedení matričních knih (kniha narození, manželství, partnerství, úmrtí) a v nich obsažených údajů
- příspěvky na péči sociálních služeb
  např. osobní údaje v informačním systému o příspěvku na péči
- nakládání s komunálním odpadem
  zejm. vedení evidence odpadů, osobní údaje osob, od kterých je vykupován odpad, kontrola a ukládání pokut

Z pohledu obecně závazných právních předpisů vystupuje subjekt, kterému je svěřen výkon státní správy, v postavení ***správce;*** jinak tomu však může být, pokud zpracování údajů je prováděno pro jinou osobu - správce, který určil účel a prostředky zpracování. U všech subjektů, které s osobními údaji na místní úrovni pracují (vedou papírové či elektronické databáze), je proto třeba provést kontrolu dodržování bezpečnosti nakládání s údaji a ověřit jejich odpovědnost v souvislosti s jejich postavením při nakládání s osobními údaji. Zatím je stále nejasné, v jakém rozsahu lze rozdělit jednotlivé povinnosti a odpovědnost dle stávající legislativy mezi odlišné role ***správce*** a ***zpracovatele***, popř. mezi dva ***společné správce***. Proto je třeba počínat si opatrně na všech úrovních.

2.1.2 Samostatná působnost

Na úseku samostatné působnosti dochází ke zpracování osobních údajů zejména v následujících oblastech:

- sociálních služeb
  např. údaje shromažďované městskou částí při zjišťování potřeb poskytování sociálních služeb osobám nebo skupinám osob na svém území

- kulturní činnost, sport, rekreace a cestovní ruch
  např. údaje z evidence povolení k výkonu umělecké, kulturní, sportovní a reklamní činnosti dětí
- základní školy, zařízení jim sloužící a předškolní zařízení
  např. dokumentace škol a rozsah osobních údajů vedený ve školní matrice
- nakládání s komunálním odpadem
  týká se odvozu a likvidace tuhých komunálních odpadů a spadají sem např. údaje osob, od kterých je svážen odpad odvoz
- zřízení jednotky dobrovolných hasičů
  např. jméno, příjmení či bydliště nových členů jednotky

V rámci samostatné působnosti vystupuje hl. m. Praha, její městské části i příspěvkové organizace v rolích ***správce*** i ***zpracovatele*** osobních údajů (tj. např. tak, že pro konkrétní činnost může být příspěvková organizace ***správcem*** a hl. m. Praha ***zpracovatelem*** osobních údajů) anebo i naopak.

2.2 PŘÍSPĚVKOVÉ A DALŠÍ ORGANIZACE

Právo zakládat, zřizovat a rušit příspěvkové organizace nebo obecně prospěšné společnosti spadá do samostatné působnosti hl. m. Prahy a jejích městských částí a děje se v rámci výše naznačených oblastí. Co do objemu významnému nakládání s osobními údaji, ke zpracování dat dochází zejména u následujících kategorií subjektů:

- domovy dětí a mládeže
  např. osobní údaje dětí a zákonných zástupců uváděné v přihlášce
- domovy pro seniory
  např. údaje o příjmech klientů, kontaktní údaje
- domovy pro zdravotně handicapované
  např. speciální požadavky osob vč. stravování a užívaných přípravků
- organizace poskytující zdravotní péči (polikliniky, nemocnice)
  např. zdravotní stav klientů, kontaktní a platební údaje, evidence receptů
- školy
  např. údaje získané při zápisu do školy, kroužky a stravování, evidence dárců/sponzorů
- divadla, muzea, galerie
  např. e-mailové adresy k rozesílání novinek/aktualit
- ostatní (např. Institut plánování a rozvoje, Lesy hl. m. Prahy, Pohřební ústav hl. m. Prahy, Správa pražských hřbitovů, Technická správa komunikací hl. m. Prahy)
  např. údaje osob využívajících kontaktní formuláře, údaje smluvních stran a jejich zástupců v případě uzavírání smluv

Ačkoli jsou příspěvkové a další organizace zřízeny hl. m. Prahou a jejími městskými částmi, mají vlastní subjektivitu a tedy i vlastní agendu nakládání s osobními údaji, v níž nejčastěji vystupují v roli ***správce*** osobních údajů. V rámci budoucích auditů a analýz zpracování osobních údajů bude třeba pro určení přesných povinností zkoumat, do jaké míry z pohledu dnešní praxe dochází ke sdílení osobních údajů mezi jednotlivými příspěvkovými organizacemi a městskými částmi či hl. m. Prahou. Pro tyto subjekty je ve smlouvách nezbytné stanovit jasná a srozumitelná pravidla pro nakládání s osobními údaji tak, aby byla vymezena jejich odpovědnost a nebylo pochyb o tom, kdo a jak má s daty nakládat.

2.3 ZAMĚSTNANCI, DODAVATELÉ

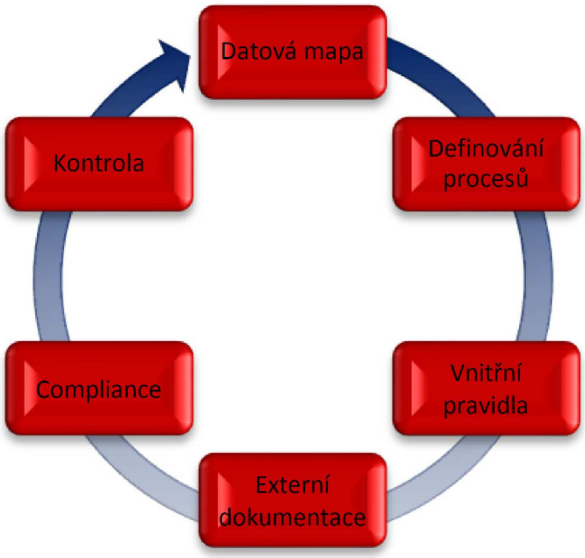
Hl. m. Praha jako zaměstnavatel a zřizovatel rovněž nakládá s osobními údaji zaměstnanců (hl. m. Prahy, městských částí či jimi zřizovaných organizací), externích pracovníků a dodavatelů zboží a služeb.

2.4 ZAPOJENÍ ZPRACOVATELŮ OSOBNÍCH ÚDAJŮ

Existují činnosti, pro které je vhodné či dokonce nezbytně nutné zajistit zpracovávání osobních údajů třetí osobou. Například marketingové a reklamní aktivity (newslettery, časopisy městských částí, ankety, soutěže, průzkumy veřejného mínění) jsou typickým příkladem tzv. outsourcingu činností na třetí osoby, které se pro potřeby uvedené činnosti stávají pověřenými zpracovateli osobních údajů a z této pozice jim vyplývají nezanedbatelné povinnosti v oblasti nakládání s osobními údaji (čl. 28 GDPR).

3. JAK SE PŘIPRAVIT

Ve vztahu ke vstupu GDPR v účinnost by hl. m. Praha, její městské části a jimi zřizované příspěvkové organizace, jako každý jiný ***správce*** nebo ***zpracovatel*** údajů, měly s ohledem na nemalý počet osobních údajů, s nimiž nakládají a které zpracovávají, provést zejména interní analýzu zpracování osobních údajů, posoudit, které povinnosti dle GDPR a v jakém rozsahu se na ně vztahují, zajistit/přijmout bezpečnostní opatření, přizpůsobit všechny interní postupy a upravit externí vztahy. Tyto kroky by měly vést k jejich budoucímu naplňování požadavků GDPR.



Navržené kroky a naznačené postupy budou mít v návaznosti na konkrétní příspěvkovou organizaci či agendu specifické znaky a obsah.

3.1 ZAJISTIT POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

- posoudit, zda bude konkrétní organizace (nejen příspěvková) potřebovat pověřence ochrany osobních údajů a zda je vhodné tuto funkci zajistit z vlastních zdrojů, nebo raději externě (čl. 37 GDPR)
- jmenovat nebo externě zajistit *nezávislého* pověřence pro ochranu osobních údajů, u něhož nedochází ke střetu zájmů (čl. 38 odst. 6 GDPR). V konfliktním postavení mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování. Lze předpokládat, že i interní auditor by mohl být v konfliktním postavení, pokud objektivně může vznikat obava, že hodnocení auditu by s ohledem na zavedené postupy při zpracování nemusely být provedeny objektivně (zpravidla tomu tak bude, ledaže organizace zavedla specifická opatření pro zpracování a hodnocení auditu oproti jinak běžným základním postupům)
- zapojit pověřence do veškerých záležitostí souvisejících s ochranou osobních údajů a poskytnout mu zdroje nezbytné k plnění jeho úkolů (čl. 38 odst. 1 GDPR) a zveřejnit jeho údaje (čl. 37 odst. 7 GDPR)

3.2 PROVÉST ZÁKLADNÍ AUDIT ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- zajistit základní audit zpracování osobních údajů, který má za cíl zmapovat faktickou situaci v organizaci – vytvoření některého z modelů tzv. „datové mapy“
- zjistit, do jaké míry se organizace GDPR dotkne, zejména jaké osobní údaje zpracovává, pro jaké účely, po jakou dobu osobní údaje uchovává, kde se zpracovává a jak riziková daná zpracování jsou

3.3 NASTAVIT VNITŘNÍ PROCESY A ZAJISTIT ODPOVÍDAJÍCÍ DOKUMENTACI

- nastavit kulturu organizace: monitoring, přezkoumání, zhodnocení postupů zpracování osobních údajů s cílem dodržení požadované zásady minimalizace zpracování a ukládání osobních údajů
- připravit si odpovídající dokumentaci: záznamy o činnostech zpracování (čl. 30 GDPR), posouzení vlivů na ochranu osobních údajů (čl. 35 GDPR)
- proškolit zaměstnance, kteří nakládají s osobními údaji, např. mají přístup do databází

3.4 REVIDOVAT SMĚRNICE A DOKUMENTY NA OCHRANU OSOBNÍCH ÚDAJŮ

- zajistit, aby byl text zásad zpracování osobních údajů či souhlasů se zpracováním v souladu s GDPR psán srozumitelným a jasným jazykem
- dodržet transparentnost a zohlednit zvláštní požadavky na srozumitelnost ve vztahu k dětem (např. grafické znázornění zásad)

3.5 ZAJISTIT BEZPEČNOST ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- zabezpečit osobní údaje po technické a organizační stránce, tj. organizačně v dokumentech určit např. přístupové role a stanovit technické prostředky k jejich zabezpečení jako např.:
    - používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob,
    - údaje v elektronické podobě uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým mají přístup pouze pověřené osoby na základě přístupových kódů či hesel,
    - zajistit dálkový přenos údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích,
    - písemné dokumenty obsahující osobní údaje uchovávat na zabezpečeném místě (uzamykatelná skříň, místnost, atd.), přičemž zároveň vést řádnou evidenci o pohybu takových písemných dokumentů,
    - nemožnost nahrávat data na soukromé USB klíče, apod.
- kategorizovat bezpečnostní opatření v závislosti na riziku zpracování
- zabezpečit přičitatelnost (stanovit pravidla pro přístup k datům (hesla a role), zajistit logování)
- zajistit mechanismus detekce incidentů

3.6 REVIDOVAT SMLUVNÍ VZTAHY

- organizace, která vystupuje v pozici ***správce***, by měla revidovat smlouvy o zpracování osobních údajů se svými zpracovateli, a to z hlediska nových požadavků kladených na tyto smlouvy dle GDPR
- organizace, která vystupuje v pozici ***zpracovatele*** osobních údajů pro správce, by měla posoudit své možnosti a schopnosti před převzetím povinností od správců

3.7 PŘIPRAVIT PROCESY, JAK REAGOVAT NA UPLATNĚNÁ PRÁVA SUBJEKTŮ ÚDAJŮ

- zavést či zrevidovat postupy, jak co nejrychleji a nejefektivněji reagovat v případě, kdy subjekt údajů uplatní vůči organizaci své právo na přístup k osobním údajům, výmaz, opravu, omezení zpracování, vznese námitku proti zpracování apod.

3.8 PŘIPRAVIT MECHANISMY PRO PŘÍPADY PORUŠENÍ OCHRANY OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ

- připravit jasné postupy pro případné porušení osobních údajů

- připravit postupy pro ohlašování incidentů ve vztahu k Úřadu pro ochranu osobních údajů i ve vztahu k subjektům údajů

3.9 CERTIFIKACE (ZEJMÉNA U DODAVATELŮ)

- sledovat nástup a případně využít GDPR předjímaných certifikovaných služeb v oblasti osobních údajů zohledňujících specifické potřeby hl. m. Prahy, tj. využívat služeb těch subjektů, jež disponují certifikací jako např. **ISO/IEC 27001** - mezinárodně platný standard, který definuje požadavky na systém managementu bezpečnosti informací, především pak řízení bezpečnosti důvěry informací pro zaměstnance, procesy, IT systémy a strategii firmy, **ISO 20000/ITIL -** mezinárodně uznávaný a rozšířený standard pro řízení a správu IT služeb, kterým organizace prokazuje vysokou úroveň řízení svých IT procesů
- především u významných zpracovatelů osobních údajů, u nichž bude nezbytné klást mimořádný důraz na bezpečnost osobních údajů, požadovat např. certifikace na ISO 27001, neprokáže-li dodavatel splnění požadavků GDPR jinak

3.10 KONTINUÁLNÍ DODRŽOVÁNÍ ZÁKLADNÍCH ZÁSAD

- u každého osobního údaje mít jasně stanovený účel jeho zpracování, který není v rozporu s právními předpisy nebo oprávněnými zájmy subjektů údajů (měnit účel v průběhu zpracování principiálně lze, ale pouze ve značně omezeném rozsahu)
- každý osobní údaj musí být pro daný účel zpracován na základě platného právního titulu/důvodu (čl. 6 GDPR) (zejména zákonné zmocnění, výjimečně pak souhlas subjektu údajů)
- zpracovávat je možné pouze osobní údaje v nejmenším možném rozsahu, který ještě postačuje ke splnění účelu zpracování (zásada minimalizace) (čl. 5 GDPR)
- je-li právním důvodem pro zpracování osobních údajů souhlas subjektu údajů, musí splňovat náležitosti dle GDPR (před udělením souhlasu náležité informování a poučení mimo jiné i o možnosti odvolání souhlasu) a udělení souhlasu musí být schopno hl. m. Praha, jeho městská část či jejich příspěvková organizace v roli ***správce*** kdykoliv prokázat (čl. 7 GDPR)
- v každém případě zpracování osobních údajů musí být subjekt údajů náležitě informován o podmínkách zpracování údajů a o svých souvisejících právech (čl. 12 GDPR)
- průběžně dbát na bezpečnost osobních údajů implementací technických a organizačních opatření adekvátních danému účelu zpracování, kategorii zpracovávaných údajů a rizikům, která mohou být s daným zpracováním spojena (čl. 25 GDPR)
- zajistit právní titul k případnému předání osobních údajů mimo EU/EHS
- zavázat osoby, které přistupují k osobním údajům, či je dále zpracovávají, dodržovat vnitřní směrnice regulující ochranu osobních údajů uvnitř organizace (směrnice a zásady ochrany osobních údajů), zajistit seznámení těchto osob s vnitřními dokumenty a jejich dodržování důsledně kontrolovat a vynucovat
- určit oddělení, týmy či jednotlivce odpovědné za jednotlivé druhy zpracování
- náležitě vyškolit zaměstnance, kteří s osobními údaji nakládají
- v případě jakýchkoliv pochybností při konkrétních zpracováních se poradit s odborníky.

4. TYPICKÝ PRŮBĚH GDPR PROJEKTU (AUDITU)

Projekty GDPR lze členit do tří základních fází, které obsahují dílčí navzájem se podmiňující plnění poradců. Nejčastěji subjekty, které se chtějí podrobit kontrole, objednávají (právní) první fázi s tím, že na další fáze najímají specializované IT konzultanty nebo je řeší svépomocí interně.

V první fázi projektů většinou dochází k provedení právní analýzy specifik zkoumaného subjektu z pohledu požadavků GDPR. Povinnou součástí každého projektu v této fázi je zmapování zpracování osobních údajů v rámci procesů zkoumaného subjektu (vytvoření tzv. datové mapy) a určení požadavků GDPR a jejich dopadů (tzv. GAP analýza) s hodnocením závažnosti dopadu a rizika plynoucího z jejich nenaplnění. První fáze přináší odpověď na otázky: *které oblasti činnosti kontrolovaného subjektu podléhají GDPR, jaké má GDPR relevantní požadavky* a *jaké bezpečnostní mezery (gaps) je nezbytné odstranit*.

Ve druhé fázi projektu dochází ke konzultacím vhodného řešení pro nakládání s osobními údaji a připomínkování a kontrole technických způsobů splnění (GAP analýzou identifikovaných) povinností, doporučených kroků a obchodních specifikací řešení v oblasti informačních technologií (IT).

Poslední (třetí) fáze pak nejčastěji slouží k revizi nové IT architektury, kontrole zavádění zvoleného technického řešení a k právní revizi či vyhotovení interních metodik, směrnic, kodexů, formulářů, obsahu webových stránek nebo vzorových souhlasů se zpracováním osobních údajů. Poslední fázi někteří poradci zakončují závěrečnou zprávou o nakládání s osobními údaji v souladu s GDPR.

Většina poradců bude pro bezchybné provedení GDPR auditu po kontrolovaném subjektu požadovat zejména:

- určení projektového manažera (kontaktní osoby)
- seznam IT systémů a programových řešení pracujících s osobními údaji a popis IT architektury
- poskytnutí veškerých existujících dokumentů souvisejících s osobními údaji (interní směrnice, politika zpracování osobních údajů, souhlasy se zpracováním osobních údajů, informace o zpracování osobních údajů obsažené ve smlouvách či obchodních podmínkách, smlouvy o zpracování osobních údajů, smlouvy o předání osobních údajů do zahraničí apod.)
- opakovaná setkání s jeho vybranými zástupci za účelem sběru informací (zejm. o existujících procesech nakládání s osobními údaji, nastavení reakcí a odpovědí na uplatnění stávajících práv subjektů údajů, hlášení případů narušení bezpečnosti osobních údajů atd.)
- kontrolu obsahové úplnosti datové mapy, na jejímž základě provádí poradce veškeré další kroky
- účast na školení (vybraných zástupců k vyplňování datové mapy, všech klíčových zástupců k představení nápravných kroků po GAP analýze atd.).

Příloha č. 1 - příklady zpracování osobních údajů v rámci vyjmenovaných příspěvkových organizací

Příloha č. 2 – vysvětlení pojmu „osobní údaj“ a „zpracování osobních údajů“

Školy

První evidence osobních údajů dětí, žáků a studentů a jejich zákonných zástupců je primárně spojena s podáním přihlášky do přijímacího řízení k přijetí do školy. Ve škole pak zejména při hodnocení dětí, žáků a studentů dochází ke sběru rozsáhlého množství údajů o jejich životě; většina těchto údajů je nezbytná ke splnění právní povinnosti školy či školského zařízení vyplývajícího ze školského zákona. Některé údaje však mohou být zpracovávány nad rámec tohoto zákona a zde je potřeba posoudit a určit, jaký další právní titul je možno využít (např. souhlas rodičů anebo jiný právní zájem).

Škola organizuje různé kroužky, sportovní aktivity, družinu, a eviduje strávníky včetně zvláštních dietárních potřeb. Za tyto akce škola přijímá peněžní prostředky (vybírá ale i různé další příspěvky např. na školní potřeby) a vede evidenci plateb, tj. i údajů, které souvisí s přijetím platby. Podobná evidence je vedena také v případě přijetí darů a peněžních prostředků od sponzorů instituce (např. sdružení rodičů a přátel školy). V rámci akcí spolufinancovaných z fondů Evropské unie školy shromažďují i další osobní údaje – například informace o postavení rodičů na trhu práce.

Škola také eviduje informace o zvláštním zdravotním stavu dětí, žáků a studentů.

Dále škola vede personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči svým zaměstnancům a pracovníkům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob.

V neposlední řadě začínají školy identifikovat děti, žáky a studenty, popř. třetí osoby při vstupu do budovy tak, aby byla zabezpečena ochrana osob nacházejících se v budově školy, a to v souvislosti Metodickým doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních – Minimální standard bezpečnosti.

Domovy dětí a mládeže

Domovy dětí a mládeže vedou evidence osobních údajů dětí a zákonných zástupců na základě přihlášky. Další evidence vzniká na základě dílčích přihlášek na konkrétní sportovní nebo kulturní aktivity, tábory, soustředění (shromažďovány jsou údaje jako např. jméno a příjmení, datum narození, rodné číslo, bydliště, škola, identifikace zdravotní pojišťovny, údaj o občanství a jiné). Konkrétně se tedy jedná o kontaktní údaje a dále informace o stravovacích návycích, zvláštním zdravotním stavu dětí (údaje o zdravotních komplikacích, zdravotním postižení, znevýhodnění a další údaje, které by mohly mít vliv na poskytování zájmového vzdělávání) a podobně. V rámci akcí spolufinancovaných z fondů Evropské unie domovy shromažďují i další osobní údaje – například informace o postavení rodičů na trhu práce.

Na základě poskytovaných služeb přijímá instituce peněžní prostředky a vede evidenci plateb, tj. i údajů, které souvisí s přijetím platby. Podobná evidence je vedena také v případě přijetí darů a peněžních prostředků od sponzorů instituce.

V rámci své činnosti zaměstnanci instituce pořizují fotografie a kamerové záznamy, které následně jsou i zpřístupňovány na internetových stránkách jednotlivých domovů dětí a mládeže.

V neposlední řadě instituce vede také personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči svým zaměstnancům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob.

Divadla, muzea, galerie

Prostřednictvím objednávkových systémů získávají tyto instituce osobní údaje návštěvníků. Pořádají různé akce a v souvislosti s nimi pak evidují osobní a kontaktní údaje účastníků. Divadla, muzea, galerie také vedou seznamy e-mailových kontaktů, na které jsou rozesílány novinky a aktuality (obchodní sdělení).

V rámci ochrany majetku jsou často pořizovány kamerové záznamy případně fotografie. Fotografie jsou následně také přístupné na internetových stránkách instituce. Na stránkách (např. národního muzea) je dostupný live stream z kamer, umístěných na budovách muzeí, galerií či divadel, přičemž tyto kamery snímají veřejně dostupná místa. Dochází tak ke zpracování a zveřejňování osobních údajů osob, které jsou kamerami zachyceny.

Instituce také vedou seznam sponzorů a evidují případné dary a sponzory; relevantní seznamy bývají zveřejňovány například on-line na stránkách jednotlivých institucí.

Divadla, muzea a galerie vedou dále personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči zaměstnancům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob. V divadlech je zejména pro mzdové a personální účely vedena evidence účinkujících, kteří mohou být i zahraničními osobami.

Domovy pro seniory

Domovy pro seniory vedou evidenci osobních údajů klientů na základě přihlášky pro přijetí do péče domova, které obsahuje kontaktní údaje o klientovi a údaje o jeho kontaktní osobě. Domovy pro seniory vedou rovněž evidenci údajů o zdravotním stavu klienta (údaje o zdravotních komplikacích, zdravotním postižení, znevýhodnění a další údaje, které by mohly mít vliv na poskytovanou péči), údaje o zdravotních přípravcích užívaných klientem, jeho lékařích nebo informace o stravovacích návycích. Tyto údaje uchovávají a zpracovávají za účelem zvýšení kvality poskytované péče a poskytování dalších nadstandardních služeb (poskytování rehabilitace, poradenství, individuálních a skupinových aktivit).

Péče o seniory jako taková nebo pouze konkrétní služby mohou být zpoplatněné a v takovém případě domovy vedou evidenci plateb – tj. údaje o přijatých platbách za poskytnuté služby a údaje o příjmech klienta. Při spoluúčasti na platbách za péči a služby (např. ze strany rodinných příslušníků) jsou sbírána data na základě souhlasu o spoluúčasti na úhradě nákladů třetí osoby. Dále domovy vedou záznamy o darech od sponzorů.

V rámci poskytovaných služeb instituce umožňují stravování. Při poskytování této služby může vznikat evidence údajů – záznamy o klientovi získané z jídelny.

V rámci své činnosti mohou zaměstnanci domovů pořizovat fotografie a kamerové záznamy, které mohou být zpřístupněny na internetových stránkách domova.

V neposlední řadě instituce vede také personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči svým zaměstnancům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob.

Domovy pro zdravotně handicapované

Domovy pro zdravotně handicapované vedou evidenci osobních údajů klientů na základě přihlášky pro přijetí do péče domova, která obsahuje kontaktní údaje o klientovi a údaje o jeho kontaktní osobě. Domovy pro zdravotně handicapované vedou evidenci údajů o zdravotním stavu klienta (údaje o zdravotních komplikacích, zdravotním postižení, znevýhodnění a další údaje, které by mohly mít vliv na poskytovanou péči), údaje o zdravotních přípravcích užívaných klientem, jeho lékařích a informace o stravovacích návycích. Tyto údaje uchovávají a zpracovávají za účelem zvýšení kvality poskytované péče a poskytování dalších nadstandardních služeb (např. poskytování rehabilitace).

Péče o zdravotně handicapované jako takové nebo pouze konkrétní služby mohou být zpoplatněné (dle zákona o sociálních službách). V tomto případě domovy vedou evidenci plateb – tj. údaje o přijatých platbách za poskytnuté služby. Dále domovy vedou záznamy o darech od sponzorů (tj. i údaje o sponzorech).

V rámci poskytovaných služeb instituce umožňují stravování. Při poskytování této služby může vznikat evidence údajů – záznamy o klientovi získané z jídelny (např. diety).

V rámci své činnosti mohou zaměstnanci domovů pořizovat fotografie a kamerové záznamy, které jsou následně také přístupné na internetových stránkách domova.

V neposlední řadě instituce vede také personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči svým zaměstnancům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob.

Organizace poskytující zdravotní péči – polikliniky, nemocnice

Primárně evidence vzniká registrací pro účely poskytování zdravotní péče. Tyto instituce vedou evidenci osobních údajů pacientů a vedou zdravotnickou dokumentaci dle zákona o zdravotních službách. V lékařských záznamech – v kartě pacienta se evidují zejména informace o zdravotním stavu, o tělesném a duševním zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb. Evidují se recepty, údaje zdravotních pojišťoven, záznamy o zakoupení léčiv nebo zdravotnických produktů, informace o testech, zkouškách, informace o nemoci, postižení, riziku onemocnění, anamnéze či léčbě. Osobními údaji jsou i údaje získané pomocí mobilních aplikací sloužících k monitorování údajů souvisejících se zdravím, kdy je monitorováno stravování, tělesná kondice či fyziologické parametry osoby.

Poskytovatel zdravotních služeb se může podílet na klinickém výzkumu, s čímž je spojeno zpracování osobních údajů jak pacientů, tak lékařů, školitelů a dalších osob podílejících se na tomto výzkumu.

Na základě poskytovaných služeb přijímá instituce peněžní prostředky a vede evidenci plateb, tj. i údajů, které souvisí s přijetím platby. Podobná evidence je vedena také v případě přijetí darů a peněžních prostředků od sponzorů instituce.

Je vedena také evidence návštěv.

Instituce vede také personální evidenci pro účely plnění pracovněprávních smluv a povinností vůči zaměstnancům dle zákoníku práce.

Ostatní specifické instituce (např. Institut plánování a rozvoje, Lesy HMP, TSK apod.)

Tyto instituce evidují osobní údaje smluvních stran, ale i například registrační údaje. Je vedena personální evidence pro plnění pracovněprávních smluv a povinností vůči zaměstnancům dle zákoníku práce. Instituce vedou také seznamy případných plateb a s nimi souvisejících údajů.

Instituce je také možné kontaktovat elektronicky vyplněním formuláře, ve kterém jsou zpracovávány osobní údaje. Některé instituce umožňují přihlášení na svých internetových stránkách, přičemž k přihlášení je nutno zadávat osobní údaje.

V rámci vzdělávacích akcí zpracovávají osobní údaje o účastnících, pořizují fotografie a kamerové záznamy, které jsou, mimo jiné, uveřejňovány na stránkách institucí.

Pohřební ústav HMP a Správa pražských hřbitovů

Tyto instituce evidují osobní údaje zemřelých a pozůstalých (v souvislosti se zajišťováním pohřbů, evidencí hrobových míst, evidencí související s provozováním veřejného pohřebiště apod.). Osobní údaje zemřelých osob jsou z velké části z ochrany osobních údajů dle současných předpisů i nařízení GDPR vyloučeny, i na ně se však vztahují některé povinnosti správců osobních údajů (zejména zabezpečení osobních údajů).

Dále tyto instituce evidují a zpracovávají například osobní údaje soutěžitelů v architektonických soutěžích. Je vedena personální evidence pro plnění pracovněprávních smluv a povinností vůči zaměstnancům dle zákoníku práce. Kromě této evidence může vznikat evidence dalších spolupracujících osob. V případě objednání služeb se evidují údaje o objednateli a záznamy o platbách a s nimi související údaje.

V rámci internetových stránek je možné kontaktovat instituce, přičemž ke kontaktování je nutné uvést osobní údaje.

Příloha č. 2 – vysvětlení pojmu „osobní údaj“ a „zpracování osobních údajů“

OSOBNÍ ÚDAJ

Za osobní údaj se považuje **jakákoli informace, která se týká fyzické osoby, pokud je možné tuto osobu na základě takové informace přímo nebo nepřímo identifikovat**. Identifikace může proběhnout zejména na základě čísla, kódu nebo určitých prvků, které jsou specifické pro konkrétní osobu. Základním znakem osobního údaje je tedy to, že znemožňuje či snižuje možnost záměny jedné fyzické osoby s jinou fyzickou osobou. Za tímto účelem pak **osobním údajem může být i několik údajů, u nichž nemusí být na první pohled patrné, že tyto údaje souvisí s konkrétní fyzickou osobou** (např. barva či značka vozidla), nicméně ve spojení s dalšími informacemi/údaji/okolnostmi mohou vést k určení konkrétní fyzické osoby. Není také rozhodné, zda konkrétní osoba pracující s osobními údaji je schopna konkrétní fyzickou osobu identifikovat, ale postačí, aby tuto identifikaci dokázala provést kterákoliv jiná (byť jen jediná) osoba (např. v případě potenciálního úniku údajů).

Za osobní údaj se naopak **nepovažují údaje anonymní či anonymizované** (tedy údaje neumožňující identifikaci fyzické osoby – např. nashromážděná statistická data).

Zvláštní skupinou osobních údajů jsou citlivé osobní údaje. Ty vypovídají například o národnostním nebo etnickém původu osoby, jejích politických postojích, členství v odborových organizacích, náboženství atd. Citlivým údajem je i informace o odsouzení za trestný čin, o zdravotním stavu anebo genetické či biometrické údaje (např. otisk prstu). Aby byl konkrétní osobní údaj z pohledu práva citlivý, je třeba, aby účelem zpracování tohoto údaje byla právě analýza či jiné použití výše uvedených „citlivých“ znaků. Přestože některé osobní údaje mohou mít citlivější povahu (např. finanční údaje), tyto nejsou považovány za citlivé osobní údaje ve výše uvedeném významu.

V návaznosti na nařízení GDPR, ve vztahu k němuž bude za několik měsíců probíhat analýza všech procesů v rámci hl. m. Prahy, mohou mezi nejčastěji zpracovávané osobní údaje v rámci činnosti hl. m. Prahy patřit zejména:

- jméno/příjmení
- bydliště
- datum narození
- rodné číslo
- fotografie
- video záznam
- audio záznam
- osobní stav
- údaj o zdravotním stavu
- e-mailová adresa
- telefonní číslo
- IP adresa
- záznamy chování na internetových stránkách (cookies apod.)
- SPZ, barva či značka vozidla
- VIN kód vozidla
- číslo OP/ŘP
- GPS záznamy ze služebního vozidla
- údaje o příjmech fyzické osoby
- otisk prstu
- podpis

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pojem zpracování představuje **jakoukoliv operaci nebo soustavu operací, která se provádí systematicky s osobními údaji, přičemž není rozhodující, zda se s osobními údaji pracuje automatizovaně nebo neautomatizovaně (tedy i manuálně)**. Obecně se bude jednat především o shromažďování, ukládání osobních údajů na nosiče informací, jejich zpřístupňování, systematické nahlížení, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování či likvidaci osobních údajů.

Nařízení GDPR považuje za zpracování v zásadě každou operaci prováděnou s osobními údaji. Následující činnosti budou tedy typickým příkladem zpracování osobních údajů:

- přijímání formulářů s vyplněnými údaji od třetích osob
- zpracování údajů ze žádostí, stížností, podnětů atd.
- zapisování údajů do evidence
- vedení evidence (obyvatel, nájemníků bytových a nebytových prostor či jakákoliv jiná evidence)
- přepisování údajů z listinné do elektronické podoby (a naopak)
- vedení spisů ve správním řízení
- nahlížení do spisů, evidencí atd.
- vyhotovování kopií osobních dokladů
- plnění pracovněprávních povinností vůči zaměstnancům (např. evidence pracovních úrazů, mzdová agenda)
- shromažďování údajů při uzavírání smluv
- vydávání voličských průkazů
- ověřování podpisů/listin