GDPR

METODIKA PRO ADVOKÁTY A ADVOKÁTNÍ KANCELÁŘE K DOSAŽENÍ SHODY S GDPR

Česká advokátní komora | Národní tř. 16 | 110 00 Praha 1 | Česká republika
tel.: 273 193 111 | e-mail: epodatelna@cak.cz | www.cak.cz | DS: n69admd

Obsah

1. ÚVOD

Nařízení Evropského parlamentu a Rady (EU) 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 (obecné nařízení o ochraně osobních údajů; dále jen jako „**GDPR**“), které nabylo účinnosti 25. května 2018, představuje základní stavební kámen v novém evropském legislativním rámci ochrany osobních údajů a rovněž první milník v chápání ochrany osobních údajů jako základního regulačního nástroje pro oblast tzv. digitální ekonomiky v EU.

Do působnosti GDPR spadá veškeré zpracování osobních údajů fyzických osob na území EU/EHP, a to bez ohledu na formu účel, cíl, právní titul, formu zpracování (automatizované/elektronické i manuální) anebo postavení osoby, která za zpracování osobních údajů odpovídá.

Přes pochopitelné odborné diskuse o tom, v jakém rozsahu se GDPR má vztahovat na povolání s garantovanou povinností mlčenlivosti (zejm. advokáti, dále též lékaři a poskytovatelé pečovatelských služeb, kněžská povolání ad.), je již nyní zřejmé, že GDPR se na tyto profese (advokáty nevyjímaje) ve významné míře vztahuje. ČAK připravila tuto metodiku (dále jen „**Metodika**“), s jejíž pomocí by měli být advokáti schopni se (většinou svépomocí) připravit na požadavky GDPR.

Účelem této Metodiky je pomoci advokátům s dosažením shody s GDPR, aniž by byly negativně dotčeny stávající postupy a doporučení zajišťující vysokou úroveň povinné mlčenlivosti (advokátního tajemství).

Cílem dokumentu je předložit praktická doporučení a příklady z každodenní praxe, která advokátům umožní dosáhnout shody s GDPR a současně být v dlouhodobém souladu s novými trendy, které GDPR představuje.

Určení Metodiky. Metodika je určena advokátům, advokátním koncipientům a zaměstnancům advokátních kanceláří (se zvláštním důrazem na samostatné advokáty).

2. POJMY

Základními pojmy GDPR v kontextu činnosti advokátní kanceláře jsou:

- **Osobní údaj (OÚ)** – jakákoliv informace, která se týká konkrétní fyzické osoby (subjektu údajů), ať už jde o identifikační a kontaktní údaje (např. jméno, příjmení, datum narození, adresa pobytu, rodné číslo, IČO/DIČ, telefonní číslo, e-mail, v podmínkách advokátní kanceláře např. číslo klienta anebo spisová značka věci), údaje o poloze, popisné údaje vypovídající o fyziologii člověka (např. výška, váha, velikost boty), informace z fotografií a kamerových záznamů, sociodemografické údaje (věk, pohlaví, rodinný stav, vzdělání, zaměstnání, příjmy a výdaje, počet dětí) nebo údaje o jeho chování a preferencích.
- **Zvláštní kategorie osobních údajů** (dříve citlivé osobní údaje) – některé osobní údaje zvlášť rizikové z pohledu možných zásahů do garantovaných práv a svobod fyzických osob, například údaje o zdravotním stavu, údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, genetické či biometrické údaje.
- **Subjekt údajů** – každá fyzická osoba, jejíž OÚ jsou zpracovávány.
- **Zpracování** – jakékoli nakládání s osobními údaji, např. shromáždění, zaznamenání, zpřístupnění, uložení, uspořádání, vyhledání, pozměnění, použití, šíření atd. U zpracování osobních údajů v rámci

advokátní kanceláře patří mezi typické příklady vedení spisové evidence (elektronické i listinné), evidence udělených plných mocí, vedení podpisových knih a ověřovacích knih, dokumentace v souvislosti s požadavky AML předpisů[1] aj., a to jak v rámci klientské agendy, tak i administrativních činností advokátní kanceláře (např. personalistika).

- **Správce** – jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; v případě výkonu advokacie každý samostatný advokát, advokátní společnost anebo sdružení.
- **Zpracovatel** – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává pro správce osobní údaje, pokud ho tím správce pověří, a pouze ve správcem stanoveném rozsahu a ke stanoveným účelům; není vyloučeno, že jedna osoba bude zároveň správcem (například ve vztahu ke svým zaměstnancům) i zpracovatelem (ve vztahu k jinému správci).
- **Společní správci** – správci, kteří společně stanoví účely a prostředky zpracování OÚ.
- **Příjemce** – jakýkoli subjekt, kterému jsou osobní údaje poskytnuty (není rozhodující, zda přímo správcem, nebo zpracovatelem na pokyn správce), v některých případech se za příjemce nepovažují orgány veřejné moci.
- **Právo vznést námitku** – je-li zpracování založeno na oprávněném zájmu správce, případně prováděno ve veřejném zájmu nebo při výkonu veřejné moci, má subjekt údajů právo kdykoli proti takovémuto zpracování vznést námitku, subjekt údajů má právo vznést námitku také proti zpracování za účelem přímého marketingu a správce má v tomto případě povinnost dotčené OÚ dále nezpracovávat.
- **ÚOOÚ** – Úřad pro ochranu osobních údajů, kontrolní a dozorový úřad dle GDPR v ČR, se sídlem Pplk. Sochora 27, 170 00, Praha 7, telefon: +420 234 665 111, web: www.uoou.cz.
- **Záznamy o činnostech zpracování** – každý správce osobních údajů je povinen vést záznamy o činnostech zpracování osobních údajů, za něž zodpovídá. GDPR předepisuje formální vedení záznamů o činnostech zpracování především pro velké organizace (nad 250 zaměstnanců). Nicméně, **vzhledem k tomu, že záznamy musí vést i každý správce a zpracovatel (bez ohledu na počet zaměstnanců), pokud**

  a) prováděné zpracování OÚ pravděpodobně představuje riziko pro práva a svobody subjektů údajů,

  b) zpracování OÚ není příležitostné, nebo

  c) zpracování zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů,

  bude se povinnost vést tyto formalizované záznamy týkat všech advokátů od samostatných advokátů – jednotlivců až po největší advokátní kanceláře. Každý poskytovatel advokátních služeb přitom musí zohlednit kontext, citlivost a rozsah vedených osobních údajů, tzn. malí poskytovatelé si vystačí se záznamy v jednodušší formě, zatímco velcí správci budou muset

[1] ČAK zveřejnila dne 26. 7. 2021 Metodiku k AML, viz https://www.cak.cz/scripts/detail.php?id=24764

zohlednit zvýšený objem a rizikovost zpracovávaných OÚ, aby byly schopny prokázat soulad s GDPR při případné kontrole ze strany ÚOOÚ.[2]

- **DPO – pověřenec pro ochranu osobních údajů** (z angl. *data protection officer*); DPO je jakýmsi interním auditorem zpracování a ochrany osobních údajů; dohlíží nad tím, že osobní údaje jsou zpracovávány a chráněny v souladu s GDPR. **Povinnost jmenovat DPO není plošná** (lze ho však ustavit dobrovolně). **Bude ho mít jen minimální počet advokátních kanceláří – především ty, které vedou specializovanou agendu dotýkající se zvláštních kategorií osobních údajů** (např. rozsáhlá praxe specializovaná na náhrady škod a újem při poskytování zdravotních služeb a lékařské péče). Blíže o DPO viz část 6.4 této Metodiky.
- **Analýza rizik** – posouzení zpracování osobních údajů s cílem zjistit, jak závažná rizika plynou ze zpracování pro práva a svobody fyzických osob, a na základě toho přijmout opatření, která tato rizika minimalizují. **Každá advokátní kancelář bude muset zpracovat analýzu rizik ve vztahu ke zpracováním osobních údajů, která provádí**. Blíže o analýze rizik viz vzor sestavy pro analýzu rizik v příloze této Metodiky.
- **DPIA** – posouzení vlivu na ochranu osobních údajů (z angl. *data protection impact assessment*); formalizovaná riziková analýza, jejímž úkolem je zjistit, zda i přes vysoká rizika zpracování osobních údajů, zjištěná v rámci zpracování záznamů o činnostech zpracování, lze tyto údaje legálně zpracovávat za použití opatření, která sníží vysoká rizika na přijatelnou úroveň. Podle dokumentu „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů“, jenž je zveřejněn na webu Úřadu pro ochranu osobních údajů, běžné *zpracování (operace zpracování) zajišťované jednotlivými advokáty a notáři (advokáti a notáři, kteří nejsou v zaměstnaneckém poměru), využívající nezbytné osobní údaje pouze k zajištění právních služeb pro subjekt údajů* nepodléhají posouzení vlivu na ochranu osobních údajů.[3]
- **Hlášení bezpečnostních incidentů** – GDPR obsahuje povinnost správce hlásit porušení zabezpečení, integrity a ztrátu osobních údajů ÚOOÚ bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o nich dozvěděl; z této povinnosti jsou vyloučeny pouze incidenty s nízkou rizikovostí pro subjekty osobních údajů. Navíc správci musí oznámit toto porušení neprodleně všem dotčeným subjektům údajů, pokud je pravděpodobné, že příslušné porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Blíže o hlášení bezpečnostních incidentů viz část 6.6 této Metodiky.

3. MINIMÁLNÍ POŽADAVKY NA SHODU ADVOKÁTA S GDPR

Vzhledem k obsahu činnosti a s tím související nutnosti evidovat osobní údaje je nezbytné, aby došlo k naplnění přinejmenším požadavků minimální shody advokáta s GDPR:

- Vypracování dokumentace osvědčující naplňování zásad zpracování, ochrany a zabezpečení osobních údajů (OÚ) zejména podle čl. 5, 6, 25 a 32 GDPR – touto dokumentací bude v podmínkách advokátních kanceláří vedle revize stávajících interních předpisů zejména vypracování pravidel IT bezpečnosti a pravidel bezpečného nakládání s dokumenty, včetně režimových a organizačních

[2] Vzor záznamu o činnostech zpracování viz část 6 Metodiky dále, příp. web ÚOOÚ https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30188

[3] Viz dokument Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů, web ÚOOÚ https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940

opatření[4], jakož i vypracování závazné dokumentace (interní směrnice) o zpracování osobních údajů. Součástí směrnice mohou být rovněž záznamy o činnosti zpracování (alternativně mohou být tyto záznamy samostatným dokumentem). Blíže viz část 6.1 této Metodiky.

- Zavedení a popis přinejmenším jednoho generického procesu reakcí na práva subjektů osobních údajů – blíže viz část 6.2 této Metodiky a vzory žádosti subjektu údajů a odpovědi na žádost, obsažené v příloze této Metodiky.
- Zavedení procesu naplňování informační povinnosti vůči subjektům osobních údajů – blíže viz vzor informačních povinností obsažený v příloze této Metodiky.
- Zavedení procesů identifikace, dokumentace a hlášení bezpečnostních incidentů na poli osobních údajů – blíže viz část 6.6 této Metodiky.
- Revize smluv s dodavateli advokátní kanceláře, kteří jsou zpracovateli osobních údajů – blíže viz část 6.3 této Metodiky.
- Systém sběru, evidence a zpracování souhlasů se zpracováním OÚ – blíže viz část 6.5 této Metodiky.

4. ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE GDPR

Celé GDPR vychází z několika obecných zásad zpracování a ochrany osobních údajů (obsažených především v čl. 5, 6, 25 a 32, dále ze zásady přístupu založeného na řízení rizik a informačního sebeurčení subjektů údajů). Tyto zásady jsou následující:

Zásada zákonnosti, korektnosti a transparentnosti znamená, že osobní údaje musejí být ve vztahu k subjektu údajů zpracovávány vždy korektně, zákonným a transparentním způsobem.

Zásada zákonnosti vyžaduje, aby osobní údaje byly zpracovávány na základě právem stanovených legitimních důvodů (právních titulů, které vymezuje čl. 6 GDPR), jimiž jsou: nezbytnost dodržení zákonné povinnosti, která se na správce vztahuje, nezbytnost pro splnění úkolů správce prováděných ve veřejném zájmu nebo při výkonu veřejné moci, nezbytnost pro plnění smlouvy, jejíž stranou je subjekt údajů, nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy, nezbytnost pro účely oprávněných zájmů nebo zpracování založené na souhlasu subjektu údajů.

Se **zásadou transparentnosti** souvisí plnění informačních povinností vůči dotčeným subjektům údajů vymezených v čl. 12 až 14 GDPR. **Advokáti se s těmito povinnostmi setkají již při uzavírání smlouvy s klientem**, v níž by mělo být pamatováno na poskytnutí informací klientům o zpracovávání jejich osobních údajů. Velmi vhodným místem pro naplnění informační povinnosti jsou rovněž webové stránky advokátní kanceláře.

Zásada účelového omezení znamená, že každé zpracování osobních údajů musí být v souladu se svým legálním účelem. Osobní údaje musejí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný. Dostatečně

[4] Pakliže takovou dokumentaci nepořídí advokát ve spolupráci s dodavatelem informačních technologií, mohou být vhodnými podkladovými materiály pro vypracování této dokumentace odborná literatura v oblasti bezpečnosti informací, kybernetické bezpečnosti, případně zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, resp. příloha č. 4 k jeho prováděcí vyhlášce č. 316/2014 Sb.

určitě stanovený účel je např. „plnění smlouvy“, „zasílání nabídek právních služeb“, „ochrana oprávněných zájmů – majetku správce“ nebo „plnění právní povinnosti“. Účel zpracování je výslovně vyjádřený, byl-li sdělen subjektům údajů. Legitimita účelu znamená, že je účel zpracování v souladu s právním řádem jako celkem, nikoliv tedy pouze v souladu s GDPR.

Zásada minimalizace údajů znamená, že je možné zpracovávat osobní údaje pouze v minimálním rozsahu, počtu operací a množství evidencí, které jsou nezbytně nutné a potřebné pro splnění příslušného účelu zpracování. Ačkoliv tato zásada neznamená, že by měla existovat výlučně a pouze jedna evidence, každý správce musí usilovat o to, aby osobní údaje nebyly shromažďovány v rozsahu, který překračuje potřeby účelu (např. pro plnění smlouvy o dodávce školení shromažďovat rodná čísla účastníků školení), zpracovávány nadbytečnými procesy a operacemi, popř. rozmnožovány do většího množství evidencí, než je nutné (např. každý zaměstnanec kanceláře si pořizuje svoji kopii spisu, aniž by pro to byly důležité provozní důvody).

Zásada přesnosti má vyjádření v povinnosti zpracovávat pouze přesná, správná a aktuální data. Znamená to, že v pravidelných časových intervalech (např. jednou za dva roky) by měla být osobní data klientů v databázi advokátní kanceláře aktualizována, např. formou dotazu klientům, aby potvrdili správnost svých kontaktních údajů, případně je opravili. Také je vhodné upravit v interní směrnici o zpracování osobních údajů mechanismy a opatření určená k řízení životního cyklu sbíraných osobních údajů a vedoucí k včasné opravě a/nebo likvidaci nepřesných osobních údajů, jakož i postupy uplatňované v rámci aktualizace osobních údajů (zejména z podnětu subjektu údajů). Pravidelnost ověřování přesnosti a aktualizace osobních údajů by měla odpovídat potenciálnímu riziku vzniku újmy. Vyšší riziko vzniku újmy lze očekávat v případě pravidelného zpracovávání osobních údajů než v případě jejich pouhého uložení.

Zásada omezeného uložení znamená povinnost uchovávat osobní údaje jen po dobu nezbytně nutnou k naplnění účelu zpracování. Tato zásada bude v praxi advokátní kanceláře aplikována a splněna především **dodržováním předepsaných archivačních lhůt klientských spisů a další dokumentace** (finanční, účetní, zaměstnanecké). V rámci přípravy na GDPR je proto velmi vhodné provést revizi všech stávajících archivačních a skartačních lhůt podle příslušných agend a revidovat v této souvislosti stávající dokumentaci (pokud advokátní kancelář implementovala např. spisové a archivační řády). Archivační (skartační) lhůty musejí být uvedeny v záznamech o činnostech zpracování osobních údajů a je nezbytné zajistit jejich dodržování. **Subjekt údajů by měl být informován o době, po kterou budou jeho osobní údaje zpracovávány**.

Zásada integrity a důvěrnosti představuje zejména povinnost zajistit bezpečné zpracování osobních údajů. Tato zásada se rovněž v praxi advokátní kanceláře aplikuje především formou dodržování kamerálních předpisů ČAK o ochraně klientských informací. Při posuzování vhodné úrovně bezpečnosti zpracování osobních údajů se zohlední zejména rizika, která představuje zpracování osobních údajů, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. **Vhodná technická a organizační opatření poměrně stručně zmiňuje čl. 32 GDPR**.[5] Standardizované postupy, vypracované za účelem zajištění náležité úrovně zabezpečení osobních údajů, případně

[5] Vhodnými vodítky pro identifikaci vhodných opatření je vedle čl. 32 GDPR i zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, popř. normy ISO a tzv. best practices v oblasti informační a kybernetické bezpečnosti.

včetně: a) pseudonymizace a šifrování osobních údajů; b) zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování; c) obnovení dostupnosti osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování, musejí být upraveny v **interní směrnici o zpracování osobních údajů a figurovat v záznamech o činnostech zpracování**.

5. SELF-ASSESSMENT

Část 6 této Metodiky je připravena tak, aby usnadnila advokátním kancelářím provést proces sebehodnocení z pohledu shody jejich činnosti s požadavky GDPR. Výsledkem tohoto sebehodnocení by měla být identifikace úkolů, které příslušná advokátní kancelář musí splnit, aby dosáhla shody s GDPR.

V části 6.1 níže je uvedena evidence zpracování osobních údajů s komentáři k vyplnění. Následně ve vzorech v příloze této Metodiky je uveden pouze pro ilustrační účely příklad vyplnění tabulky evidence zpracování osobních údajů fiktivní malé advokátní kanceláře. Vyplněním tabulky v tomto bodě by advokátní kanceláře měly získat základní evidenci o zpracování osobních údajů, které provádějí.

V části 6.2 je obsažen popis práv subjektů údajů, které advokátní kancelář musí být připravena vyřizovat. V příloze této Metodiky jsou pak obsaženy vzory žádosti subjektu údajů a odpovědi na žádosti. Advokátní kanceláře si tedy mohou ověřit, nakolik tyto požadavky splňují, resp. čím musí doplnit své stávající procesy k dosažení shody s GDPR v tomto ohledu.

V části 6.3 uvádíme příklady vzorových ustanovení do smluv s dodavateli – zpracovateli osobních údajů.

V části 6.4 si advokátní kanceláře budou moci ověřit, zda mají, či nemají povinnost jmenovat DPO (pověřence pro ochranu osobních údajů).

Část 6.5 pomůže advokátním kancelářím zkontrolovat si své souhlasy se zpracováním osobních údajů pro případy, kde je souhlas se zpracováním osobních údajů nutný.

Konečně na základě informací v části 6.6 budou advokátní kanceláře moci začlenit do svých interních procesů hlášení a oznamování bezpečnostních incidentů.

6. ZÁKLADNÍ VZOROVÁ INTERNÍ SMĚRNICE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Cílem této části Metodiky je připravit ve snadno srozumitelné formě základ interní směrnice, popisující postupy ochrany zpracovávaných osobních údajů při advokátní činnosti (dále jen „**Vzorová směrnice**“). Tato část **je určena zejména pro samostatné advokáty a má sloužit jako vzor** (základní vzorová osnova), který mohou samostatní advokáti sami doplnit o informace odpovídající jejich praxi, případně vybrat z nabízených variant, a dospět tak snadno a rychle k vytvoření vlastní interní směrnice.

Pro středně velké a velké advokátní kanceláře může tato část sloužit jako zdroj inspirace při vypracování vlastní interní směrnice, která vzhledem k rozsahu a variabilitě činností bude s velkou pravděpodobností vyžadovat podrobnější úpravu, než kterou poskytne Vzorová směrnice v této Metodice.

Vzorová směrnice má následující části:

6.1 Záznamy o činnostech zpracování

#	Kategorie a charakteristiky zpracování osobních údajů	Komentáře pro vyplnění
1.	Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů [článek 30 odst. 1 písm. a) GDPR]:	Uveďte jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů.
2.	Identifikace příslušných zpracování osobních údajů [článek 30 odst. 1 písm. b) GDPR]:	Uveďte seznam všech zpracování osobních údajů, které provádíte, podle hlavních kategorií: (i) klientská agenda; (ii) zaměstnanci a spolupracující advokáti; (iii) provoz AK, daně a účetnictví (dodavatelé); (iv) obchod a marketing, komunikace online; (v) ostatní.
3.	Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají [článek 30 odst. 1 písm. b) GDPR]?	Uveďte pro každé zpracování osobních údajů účel (cíl, smysl zpracování) a rovněž právní titul zpracování (půjde zejména o plnění smlouvy se subjektem a plnění zákonných povinností; v případě právní povinnosti doporučujeme uvést i odkaz na příslušný právní základ); více viz zásada zákonnosti v části 4 výše. Tuto část lze sloučit s předchozím bodem ve formátu: Zpracování – Účel – Právní titul.
4.	Jaké osobní údaje jsou zpracovávány v rámci zpracování [článek 30 odst. 1 písm. c) GDPR]?	Pro každé zpracování uveďte všechny kategorie osobních údajů, které zpracováváte.
5.	Z jakých zdrojů jsou osobní údaje získány [(článek 30 odst. 1 písm. c) GDPR]?	Uveďte všechny subjekty, od nichž získáváte osobní údaje, které v rámci své činnosti zpracováváte. Půjde jak o subjekty údajů (klienti ve vztahu ke svým vlastním osobním údajům, zaměstnanci, aj.), tak o třetí strany (soudy, klienti ve vztahu ke svědkům, aj.).
6.	Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích:	Uveďte všechny kategorie osob a organizací, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích.
7.	V jakém termínu a jak se osobní údaje likvidují [článek 30 odst. 1 písm. f) GDPR]?	Uveďte pro každé zpracování osobních údajů archivační a skartační lhůtu. Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (typicky spisový plán anebo archivační/skartační řád).
8.	Jakým způsobem se osobní údaje aktualizují [článek 30 odst. 1 písm. g) GDPR]?	Uveďte způsob aktualizace osobních údajů – viz zásada přesnosti v části 4 výše (např. obdržením informace od klienta o změně kontaktních údajů aj.).

#	Kategorie a charakteristiky zpracování osobních údajů	Komentáře pro vyplnění
		Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. spisový plán anebo směrnice o zpracování osobních údajů).
9.	Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová úložiště) provádějí zpracování [článek 30 odst. 1 písm. g) GDPR]?	Uveďte podrobně, jaké listinné evidence a IT systémy využíváte pro svou činnost a jejich vazbu na konkrétní zpracování (tzn. které evidence/IT systémy provádějí jaké zpracování osobních údajů). Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis anebo dokumentaci informačního prostředí (např. spisový plán, popis IT systémů, směrnici o zpracování osobních údajů).
10.	Je prostředí AK pravidelně bezpečnostně testováno (zejm. IT systémy)? Interně nebo externími konzultanty? [článek 30 odst. 1 písm. g) GDPR].	GDPR klade velký důraz na bezpečnost zpracování osobních údajů. Vaše IT systémy by měly být bezpečnostně testovány – interně nebo externě. V závislosti na objemu zpracovávaných osobních údajů je třeba zvolit délku časového období mezi dvěma testy. Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu).
11.	Jak je zajištěna bezpečnost předání dat při klientské komunikaci [článek 30 odst. 1 písm. g) GDPR]?	Uveďte, jak řešíte komunikaci citlivých klientských informací a dále např. jak zabezpečujete předání údajů o zaměstnancích externí účetní firmě (např. heslování, šifrování). Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu anebo směrnici o zpracování osobních údajů).
12.	Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany [článek 30 odst. 1 písm. g) ve spojení s článkem 28 GDPR]?	Uveďte, zda vaši dodavatelé, kteří mohou mít přístup ke zpracovávaným osobním údajům (např. účetní agentura nebo firma spravující váš webový systém,) mají uzavřeny smlouvy o zpracování osobních údajů. Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu anebo směrnici o zpracování osobních údajů).
13.	Je zajištěna nevratná likvidace dat v rámci databázového systému [článek 30 odst. 1 písm. g) GDPR]?	Uveďte, zda na konci životního cyklu příslušného zpracování osobních údajů je váš IT systém schopný nevratně osobní údaje vymazat.
14.	Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich data, která jsou zpracovávána v rámci zpracování?	Uveďte, zda máte zaveden interní proces vyřizování žádostí subjektů údajů ve vztahu k právům subjektů údajů – viz část 6.2 níže, a jakou formou postupujete (např. odkaz na formuláře na vašem webu nebo v listinné podobě). Rovněž je potřeba vymezit, v jakých situacích jsou práva subjektů omezována a z jakých titulů (např. nevydání informací protistraně apod.).

#	Kategorie a charakteristiky zpracování osobních údajů	Komentáře pro vyplnění
15.	Poskytují se oprávněným subjektům údajů předepsané informace, zejména o: - rozsahu a účelu zpracování, - způsobu zpracování osobních dat, komu mohou být osobní údaje zpřístupněny?	Uveďte, kde a jakou formou poskytujete předepsané informace pro subjekty údajů.
16.	Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě [článek 30 odst. 1 písm. g) GDPR]?	Uveďte, jaká bezpečnostní opatření používáte pro zajištění bezpečnosti zpracovávaných osobních údajů (provozní opatření, IT opatření). Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. bezpečnostní normu).
17.	Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí [článek 30 odst. 1 písm. e) GDPR]?	Uveďte, zda jsou vámi zpracovávané osobní údaje přenášeny do zahraničí nebo přístupné ze zahraničí. Více viz část 7 níže.
18.	Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům [článek 30 odst. 1 písm. g) GDPR]?	Uveďte, zda jsou pracovníci vaší kanceláře proškoleni o GDPR a zásadách ochrany osobních údajů. Dále uveďte, zda pracovníci vaší kanceláře, kteří nemají zákonnou povinnost mlčenlivosti ze zákona o advokacii (např. váš IT expert), mají smluvní závazek mlčenlivosti ve vztahu ke zpracovávaným osobním údajům, k nimž mají přístup.

6.2 Vyřizování žádostí a stížností subjektů údajů

GDPR obsahuje řadu práv subjektů údajů. Advokátní kanceláře musejí zajistit hladký výkon těchto práv subjekty údajů. To bude pravděpodobně jedna z priorit ÚOOÚ při kontrolách shody s GDPR. Pro účely výkonu práv subjektů údajů lze proto uvést **dvě základní doporučení**:

- Advokáti musejí pro účely shody s GDPR zajistit hladký výkon práv subjektů údajů, např. prostřednictvím online formulářů na svých webech nebo v listinné podobě přístupné na recepci apod.
- Vyřizování všech žádostí subjektů údajů musí být v souladu s předpisy o advokacii, tzn. nesmí být ohroženy zásady a principy výkonu advokacie, zejména povinnost mlčenlivosti vyplývající z § 21 zákona o advokacii a další povinnosti vyplývající ze zákona, etického kodexu a dalších kamerálních norem. GDPR nijak tyto povinnosti advokátů nesnižuje a nemění.

Prolínání obou výše popsaných principů musí být v advokacii vedeno prioritou ochrany práv klienta. Z tohoto důvodu se kladné vyřizování žádostí subjektů údajů bude týkat především žádostí klientů (včetně bývalých), popř. zaměstnanců a osob v obdobném postavení. **Vůči třetím osobám (zejm. protistrany a jejich zástupci, účastníci řízení a jednání, svědci a poškození v trestních věcech, osoby úřední apod.) je možnost advokátů poskytovat informace a naplňovat práva subjektů prakticky vyloučena povinnostmi řádného výkonu advokacie; advokát bude muset takové žádosti subjektů odmítat**. Vzhledem k šíři advokátní mlčenlivosti přitom advokát nebude v řadě případů moci vyhovět

právu subjektu ani částečně, neboť nejenže nebude moci poskytnout konkrétní informace o zpracování, potažmo kopie záznamů, ale ani potvrdit, že nějaké informace zpracovává, anebo identifikovat jejich původ.

Ve všech ostatních případech by však měl advokát postupovat tak, aby bylo uplatnění práv subjektu co nejjednodušší a nejefektivnější. Usnadnit subjektům údajů výkon jejich práv lze dále např. implementací standardizovaných procesů (postupů) zakotvených v interních předpisech a uplatňovaných v případě podání příslušné žádosti subjektem údajů, jakož i ustanovením veřejně přístupného jednotného kontaktního místa pro uplatnění nároků subjektů údajů. Důležitý je rovněž pravidelný audit výkonu činností regulovaných GDPR, evidovaná kontrola organizačních opatření a činností zpracovatelů osobních údajů. Je-li jmenován pověřenec pro ochranu osobních údajů, vykonává v rámci činnosti správce osobních údajů výše uvedený audit, dohled a další kontrolní činnosti.

Elektronické žádosti. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob. Vždy je třeba ověřit identitu toho, kdo žádost v elektronické formě podal, aby se informace nedostaly neoprávněným osobám (způsob a míra ověření by měly odpovídat kontextu, rozsahu a citlivosti požadované informace). K ověření je možné použít např. telefon nebo SMS klientovi, výjimečně lze požadovat i osobní identifikaci.

Lhůta. Informace musí být poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení.

Poplatek. Zásadně platí, že informace se poskytují bezplatně. Pouze v případě, pokud jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce. Zneužitím nelze a priori rozumět výkon práv subjektu údajů.

Níže uvádíme stručné informace o jednotlivých právech. V příloze jako jeden ze vzorů uvádíme vzor žádosti a odpovědi na žádost.

6.2.1 Právo na přístup

Přístupem k osobním údajům se rozumí právo subjektu údajů získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování,
- kategorie dotčených osobních údajů,
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
- plánovaná doba, po kterou budou osobní údaje uloženy,
- že má právo požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
- že má právo podat stížnost u dozorového úřadu,
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
- o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Pokud správce o fyzické osobě žádné údaje nezpracovává, poskytuje se informace, že osobní údaje tazatele nejsou předmětem zpracování osobních údajů ze strany správce.

Praktické dopady na činnost advokátů. Ve vztahu ke klientům lze jen doporučit, aby advokáti na žádosti klientů o přístup k osobním údajům reagovali vstřícně a poskytli alespoň hlavní kategorie osobních údajů, které advokát zpracovává. I když právní úprava umožňuje informace neposkytnout a žádost subjektu zamítnout s odkazem na to, že mu již všechny informace byly poskytnuty, **proaktivní postoj k žádostem vlastních klientů nepochybně lépe vyhoví požadavkům GDPR a výrazně eliminuje rizika případných kontrol ze strany ÚOOÚ**.

Ve vztahu k žádostem o přístup, týkajících se klientských spisů a podaných jinými osobami než klientem, bude nezbytné tyto žádosti zamítnout s odkazem na existující povinnost mlčenlivosti, tj. neposkytovat ani informaci, zda kancelář osobní údaje příslušného subjektu údajů zpracovává, či nikoliv. Podotýkáme, že **i zamítnutí žádosti musí být vyřízeno ve stanovené lhůtě**.

6.2.2 Právo na výmaz

Právo na výmaz představuje povinnost správce zlikvidovat osobní údaje, které o žadateli zpracovává, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovávány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

Výše uvedené podmínky se neuplatní, pokud je zpracování OÚ nezbytné:

a) pro **určení, výkon nebo obhajobu právních nároků**;

b) pro výkon práva na svobodu projevu a informace;

c) pro **splnění právní povinnosti**, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;

d) z důvodu veřejného zájmu v oblasti veřejného zdraví podle GDPR;

e) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle GDPR, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování.

Praktické dopady na činnost advokátů. V naprosté většině případů žádostí o výmaz v souvislosti s vedením klientského spisu bude třeba je odmítnout s odkazem na určení, výkon nebo obhajobu právních nároků, resp. na plnění právních povinností vyplývajících ze zákona o advokacii nebo v souvislosti s ním.

6.2.3 *Právo na přenositelnost*

Právo na přenositelnost představuje právo subjektu údajů získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, a to v případě, že zpracování osobních údajů je založeno na souhlasu nebo na smlouvě a zpracování se provádí elektronicky (kumulativní podmínky).

Při výkonu svého práva na přenositelnost má žadatel – subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

Praktické dopady na činnost advokátů. V případě elektronického vedení spisu je možné, že klient uplatní právo na přenositelnost v případě přechodu k jinému advokátovi.

6.2.4 *Právo na opravu nebo doplnění*

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů.

Pokud se správce domnívá, že zpracovávané osobní údaje jsou přesné, informuje o tom žadatele s odůvodněním.

Praktické dopady na činnost advokátů. Toto právo se samozřejmě uplatňuje již nyní v rámci vedení klientského spisu, kdy jsou nesprávné nebo neaktuální údaje o klientech průběžně opravovány a aktualizovány. Postup je však vhodné standardizovat v interní směrnici na ochranu osobních údajů.

6.2.5 *Další práva subjektů údajů*

GDPR obsahuje i další práva subjektů údajů, a to právo na omezení zpracování a právo podat námitku proti automatizovanému rozhodování, přičemž tato práva budou mít pravděpodobně jen omezené uplatnění v advokacii.

Ve vztahu k těmto právům odkazujeme na vzor žádosti subjektu údajů a odpovědi na žádost uvedený v příloze této Metodiky.

6.3 Revize smluv s dodavateli

Většina advokátů musí revidovat smlouvy se svými dodavateli a odběrateli služeb (např. poskytovatelé informatických služeb – dodavatelé software, externí účetní, daňové a auditorské společnosti, vymáhací agentury apod.). Dodavatelé velmi často v rámci své činnosti zpracovávají osobní údaje na základě pokynů advokátů a jsou tedy koncovými zpracovateli osobních údajů, s nimiž musejí mít advokáti coby správci uzavřené písemné smlouvy o zpracování osobních údajů, které obsahově vyhoví čl. 28 odst. 3 GDPR. Vzor základní smlouvy o zpracování osobních údajů tvoří přílohu této Metodiky.

Advokáti by měli ve smlouvách se svými dodavateli – zpracovateli osobních údajů dohodnout následující:

- Specifikovat osobní údaje, které jsou zpracovávány (např. zpracování mezd zaměstnanců advokáta)

- Uvést účel zpracování osobních údajů (např. zajišťování údržby IT systému kanceláře). Tímto účelem je omezen rozsah zpracování osobních údajů dodavatelem.
- Uvést závazek zpracovatele zpracovávat osobní údaje v souladu s příslušnými právními předpisy, smlouvou nebo pokyny advokáta vydanými v souladu s příslušnými právními předpisy. Nebude-li dodavatel moci z jakýchkoli důvodů zajistit dodržování zákonných povinností či pokyny advokáta, zavazuje se o tom advokáta neprodleně informovat.
- Uvést povinnost dodavatele a) zpracovávat pouze osobní údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu, b) nesdružovat osobní údaje, které byly získány k rozdílným účelům či c) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování.
- Uvést povinnost dodavatele přijmout před zpracováním osobních údajů odpovídající organizační a technická bezpečnostní opatření pro zajištění ochrany osobních údajů. Tato opatření zahrnují pro malé advokátní kanceláře přinejmenším zabezpečený přístup do prostor, v nichž probíhá zpracování osobních údajů, přístup k osobním údajům jen pro vybrané pracovníky dodavatele, kteří tento přístup potřebují pro účely plnění smlouvy, aj.
- Uvést závazek dodavatele proškolit své zaměstnance a další případné zástupce, kteří zpracovávají osobní údaje, o jejich povinnosti (trvající i po skončení zaměstnání nebo příslušných prací) zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.
- Uvést závazek dodavatele neprodleně oznamovat advokátovi veškeré případy náhodného nebo neoprávněného přístupu k osobním údajům.

Lze doporučit, aby advokáti vybírali své dodavatele také podle toho, jak dokáží plnit povinnosti ochrany osobních údajů podle GDPR.[6] Současně by advokáti měli v přiměřených lhůtách pravidelně kontrolovat plnění závazků dodavatelů podle uzavřených smluv o zpracování osobních údajů. Zápisky z takových kontrolních dnů budou sloužit k doložení úsilí advokáta plnit své povinnosti správce osobních údajů při případné kontrole ÚOOÚ. **Postupy a harmonogram kontrol plnění závazků dodavatelů podle uzavřených smluv o zpracování osobních údajů je třeba standardizovat v interní směrnici na ochranu osobních údajů**.

6.4 Pověřenec pro ochranu osobních údajů (DPO)

GDPR zavádí pro některé správce a zpracovatele osobních údajů povinnost ustavit a obsadit funkci tzv. pověřence pro ochranu osobních údajů (DPO), který plní funkci koordinátora a supervizora ochrany osobních údajů. GDPR uvádí několik charakteristických situací, kdy správci nebo zpracovatelé jsou povinni jmenovat DPO, v čl. 37.[7]

[6] Někteří dodavatelé služeb mohou mít zájem nahradit smlouvu jednostranným Prohlášením/osvědčením o shodě systémů/služeb s GDPR. Ačkoliv je tento přístup jednodušší a pro advokáta coby příjemce služby méně pracný, překládaná prohlášení ne vždy naplňují obsahové požadavky čl. 28 odst. 3 GDPR. ČAK proto doporučuje, aby advokáti se svými zpracovateli uzavírali standardní smlouvy, v nichž budou vymezena i práva a povinnosti strany správce.

[7] Povinnost funkci ustavit vzniká u správců a zpracovatelů, u kterých lze předpokládat vyšší pravděpodobnost výskytu nestandardních jevů při zpracování osobních údajů (např. z důvodu rozsahu anebo citlivosti údajů). Ostatní správci a zpracovatelé mohou funkci ustavit dobrovolně, v případě výkonu advokacie by však takový postup měl podléhat rigorózní analýze přínosů a rizik.

Pro advokátní kanceláře bude povinné jmenování DPO spíše výjimkou. Bude to na základě následující podmínky GDPR:

Spočívají Vaše hlavní činnosti v rozsáhlém zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů?

Zvláštní kategorie osobních údajů jsou (jak je vysvětleno v části 1 Metodiky) údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

Měřítka toho, kdy je zpracování osobních údajů rozsáhlé, GDPR nestanoví a ani ve výkladové praxi nejsou zatím nijak ustálena, a budou se dále upřesňovat. Podle *Pokynů týkajících se pověřenců pro ochranu osobních údajů* skupiny WP29 (WP 243 rev.01, verze ze dne 5. 5. 2017) naplní měřítka zpracování rozsáhlé objemem a strukturou osobních údajů, zeměpisným anebo časovým rozsahem. V podmínkách tuzemské advokacie dle názoru ČAK naplní tyto požadavky jen advokátní kanceláře specializující se na skutečně rozsáhlou právní pomoc (zejména v počtu věcí, objemu údajů a soustavnosti zpracování) v agendách, při nichž imanentně a ve velkém dochází ke zpracování osobních údajů zvláštních kategorií (v oblasti trestního práva, spotřebitelské spory, náhrada škod a újem na zdraví). Pro všechny jiné poskytovatele advokátních služeb platí, že DPO nebudou velmi pravděpodobně muset jmenovat. Zpracování OÚ velkého rozsahu je definováno v dokumentu *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů*, jehož aktuální verze je zveřejněna na webu Úřadu pro ochranu osobních údajů.[8]

K výše uvedenému je třeba dodat, že soulad postupů a procesů s GDPR v rámci činnosti správce není odpovědností DPO, nýbrž je povinností a odpovědností správce, resp. zpracovatele osobních údajů. DPO nesmí určovat nebo závazně schvalovat účely nebo prostředky zpracování osobních údajů. V takovém případě může činnost DPO směřovat ke kontrole vlastní činnosti, čímž dochází k výraznému střetu zájmů. Správce je proto vždy povinen zajistit, aby byla agenda (administrativní činnosti) související s vyřizováním záležitostí regulovaných GDPR vedena v souladu se standardizovaným postupem a související odpovědnost byla svěřena konkrétní osobě odlišné od DPO.

6.5 Souhlasy subjektů údajů se zpracováním osobních údajů

Advokátní kanceláře budou ve své praxi využívat souhlasy subjektů údajů se zpracováním jejich osobních údajů spíše omezeně, protože většina zpracování osobních údajů probíhá na základě jiných právních důvodů – zejména jako plnění ze smlouvy a plnění zákonných povinností. Příkladem toho, kdy advokát zpracovává osobní údaje na základě souhlasu, může být situace, kdy by advokát chtěl oslovovat veřejnost informacemi z určité zájmové oblasti práva, jíž se soustavně věnuje (rozesílka newsletterů splňující etické standardy reklamy na právní služby advokátů). V takovém případě musí advokát nejdříve získat souhlas spotřebitele – potenciálního klienta se zasláním příslušného sdělení.

Žádost o souhlas musí být konkrétně formulována a musí být doprovázena informacemi o účelu a prostředcích zpracování osobních údajů, o tom, s kým budou osobní údaje sdíleny, jak budou zabezpečeny a jaká práva má klient ve vztahu k svým údajům – viz vzor informačních povinností v příloze této Metodiky.

[8] https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/archiv=1&p1=3938

Souhlas může subjekt údajů kdykoliv odvolat. Souhlasy je nutné interně evidovat, přičemž tato evidence musí být systematická a přehledná (s vyznačením doby, po kterou jsou osobní údaje na základě souhlasu zpracovávány). Z tohoto důvodu se doporučuje zpracování založené na souhlasu subjektů údajů využívat minimálně.

6.6 Hlášení bezpečnostních incidentů

GDPR klade velký důraz na systematickou ochranu a zabezpečení osobních údajů. GDPR zavádí povinnost jednak hlásit bezpečnostní incidenty ÚOOÚ, a v případě, že hrozí rizika pro práva a svobody dotčených subjektů údajů, také tyto incidenty neprodleně oznamovat těmto subjektům údajů.

Nařízení GDPR definuje bezpečnostní incidenty jako případy porušení zabezpečení osobních údajů, tedy velmi široce. Spadají sem nejenom přímé útoky na zpracovávaná data zvenčí anebo zevnitř (ať již úmyslné, jako je „vynesení" informací, anebo nedbalostní, jako je např. smazání části spisu v IT systému), ale i celá řada drobnějších a méně nápadných situací, kdy advokát ztratí kontrolu nad daty, která spravuje – např. i ztráta nezabezpečeného mobilního telefonu s kontakty na klienty anebo notebooku se spisovým materiálem.

Hlášení bezpečnostních incidentů je povinné vždy, ledaže je nepravděpodobné, že by konkrétní porušení bezpečnosti mělo za následek riziko pro práva a svobody fyzických osob (např. ztráta zaheslovaného mobilního telefonu anebo krádež notebooku, jehož disk je standardně šifrován). Bohužel prozatím není k dispozici přesnější vodítko k určení, které případy se musí ÚOOÚ hlásit, a které ne.[9] Vždy je proto vhodné provést předběžné posouzení existujícího nebo potenciálního rizika a vyhodnotit jeho závažnost pro práva a svobody fyzických osob.

Jako příklad velmi závažného porušení bezpečnosti zpracovávaných osobních údajů je možné uvést ztrátu klientských spisů (ve fyzické i elektronické podobě) nebo zjištěný neoprávněný přístup ke klientským osobním údajům, které advokáti zpracovávají. Takovéto bezpečnostní incidenty bude potřeba ohlásit ÚOOÚ i dotčeným subjektům údajů. Jde ovšem o dosud zcela nevyjasněnou problematiku zejména s ohledem na povinnost mlčenlivosti advokátů – advokát by v žádném případě neměl hlásit zjištěný bezpečnostní incident bez vyhodnocení, které informace poskytnout může a které nikoliv.

Přestože ne každé porušení zabezpečení bude nutné hlásit dozorovému úřadu anebo subjektu údajů, je potřeba jej vždy zaznamenat do evidence takovýchto porušení, kterou musí mít každý správce osobních údajů.

Každý advokát by měl mít jako součást Směrnice vypracovaný postup řešení bezpečnostních incidentů. Tento postup zahrnuje nejen neprodlené hodnocení incidentu a jeho ohlášení ÚOOÚ a případně dotčeným subjektům údajů, ale také co nejrychlejší řešení incidentu a přijetí opatření k tomu, aby se, pokud možno podobný bezpečnostní incident nemohl opakovat.

7. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Při předávání osobních údajů do zahraničí do zemí mimo EU je třeba postupovat podle předepsaných postupů v GDPR. V podstatě platí následující doporučení:

[9] Na webu ÚOOÚ je k dispozici stručný návod a formulář k ohlášení porušení zabezpečení osobních údajů, viz https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5020&n=poruseni%2Dzabezpeceni&p1=5855

- Předávání zahrnuje nejen aktivní komunikaci osobních údajů, ale rovněž jejich zpřístupnění, např. formou přístupových práv k databázi.
- Pokud je předávání osobních údajů v rámci EU anebo EHP, nemusí se provádět žádné zvláštní postupy a data lze předat stejně, jako by se jednalo o předání v rámci ČR.
- Pokud jde o předání mimo EU, je třeba zkontrolovat, zda se jedná o zemi, která dle rozhodnutí Evropské komise poskytuje dostatečnou ochranu osobních údajů, a tam platí stejný režim jako pro předání v rámci EU. K 31. 7. 2021 mezi takové státy patřily Faerské ostrovy, Jersey, Ostrov Man, Guernsey, Argentina, Švýcarsko, Uruguayská republika, Andorra, Nový Zéland a Japonsko. U několika dalších států, např. Izrael, Kanada nebo USA platí zvláštní režim – více informací lze nalézt na webových stránkách ÚOOÚ.
- Pokud jsou osobní údaje předávány do jiných než výše uvedených zemí, lze využít tzv. standardních smluvních doložek přijatých Evropskou komisí. Jde o předepsanou textaci smluvních ustanovení mezi správcem/zpracovatelem ze země EU a správcem/zpracovatelem mimo EU. Při použití těchto předepsaných smluvních ustanovení není nutné žádat o souhlas ÚOOÚ s přenosem dat do zahraničí; texty všech standardních smluvních doložek jsou k dispozici na webu ÚOOÚ.

Navíc k výše uvedeným možnostem postupu existují další možnosti, které jsou podrobně popsány na webu ÚOOÚ.

8. POSTUP PŘI KONTROLE ÚOOÚ

Tato část Metodiky se zaměřuje na praktická doporučení, jak postupovat při kontrole ze strany ÚOOÚ, týkající se shody činnosti advokáta nebo advokátní kanceláře s GDPR.

Rozsah kontrolních pravomocí ÚOOÚ coby dozorového úřadu ve vztahu k advokátům je předmětem národní legislativy (viz níže).

ÚOOÚ jakožto dozorový úřad má dle čl. 58 odst. 1 písm. a) GDPR pravomoc nařídit správcům a zpracovatelům zpřístupnění všech informací nezbytných pro výkon kontrolní činnosti. Pravomoci ÚOOÚ ve vztahu k advokátům byly i předmětem judikatury Nejvyššího správního soudu (viz např. rozsudek NSS č. j. 2 As 21/2011-166), z níž vyplývá, že ÚOOÚ může v některých případech (v předmětné věci rozsáhlé vymáhání pohledávek) vykonávat svou kontrolní pravomoc i ve vztahu k advokátům, a to přímo. ČAK je nicméně toho názoru, že kontrolní pravomoc ÚOOÚ nesmí prolamovat zvláštním zákonem uloženou a ústavně garantovanou povinnost mlčenlivosti advokáta.

ČAK se vzhledem k výše uvedenému domnívá, že by kontrola ÚOOÚ měla být především zaměřena na ověření toho, zda kontrolovaný advokát:

- **plní informační povinnosti vůči subjektům údajů, jejichž data zpracovává;**
- **pořídil a udržuje povinnou dokumentaci (zejména záznamy o činnostech zpracování dle čl. 30 a dokumentaci prokazující naplnění zásad zpracování a ochrany osobních údajů dle čl. 5, 6, 25 a 32 GDPR);**
- **umožňuje hladký výkon práv subjektů údajů (s přihlédnutím k výše popsaným omezením);**

- **přijal odpovídající bezpečnostní opatření k zajištění bezpečnosti zpracovávaných osobních údajů;**
- **má přehledný systém evidence zpracovávaných osobních údajů.**

Výše uvedené by měl být každý advokát schopen doložit i bez toho, aby kontroloři ÚOOÚ měli přístup k jednotlivým klientským spisům (zejména pomocí dokumentace, jako je směrnice advokátní kanceláře; viz část 5 této Metodiky). **ČAK zastává právní názor, že vzhledem k povinnosti mlčenlivosti nesmí advokát v žádném případě vydat jednotlivý klientský spis ke kontrole ÚOOÚ.**

Otevřenou otázkou zůstává národní legislativa a následná aplikační praxe ÚOOÚ a soudů. Ustanovení § 58 odst. 1 a 2 zákona o zpracování osobních údajů[10] opravňuje ÚOOÚ se seznamovat se všemi informacemi nezbytnými pro plnění konkrétního úkolu, což platí i pro informace chráněné povinností mlčenlivosti podle jiného právního předpisu. S informacemi chráněnými povinností mlčenlivosti podle zákona o advokacii je ÚOOÚ oprávněn se seznamovat **pouze za přítomnosti a se souhlasem zástupce ČAK.**

Minimálně v počátečním období plánuje ČAK, že zástupce ČAK bude přítomen u každé kontroly advokáta ze strany ÚOOÚ. Proto nás laskavě neprodleně informujte, jakmile obdržíte oznámení o kontrole ze strany ÚOOÚ. Oznámení o chystané kontrole z ÚOOÚ obsahuje obvykle informace o tom, jaké dokumenty ÚOOÚ požaduje ke kontrole připravit. Doporučujeme zvážit, zda je čas mezi doručením oznámení a datem kontroly dostatečný pro přípravu advokátní kanceláře na kontrolu. Pokud potřebujete víc času, doporučujeme požádat ÚOOÚ o delší čas na přípravu.

Kontroloři v některých případech požadují kopie dokumentů, aby je mohli prověřit mimo advokátní kancelář. V žádném případě nedoporučujeme tímto způsobem poskytovat výpisy týkající se klientských spisů. Vždy je třeba pořídit podrobný seznam předaných kopií a nechat si jej potvrdit od kontrolora.

Z každého jednání s kontrolory doporučujeme si vyžádat zápis.

vedení České advokátní komory

Průběžně aktualizovanou vzorovou dokumentaci najdete na webových stránkách ČAK (http://www.cak/cz).

Na webových stránkách rovněž najdete přehled často kladených dotazů a odpovědí k problematice GDPR v advokacii. ČAK sbírá Vaše dotazy do této rubriky na e-mailové adrese **gdpr@cak.cz**.

[10] Zákon č. 110/2019 o zpracování osobních údajů, ve znění pozdějších předpisů.

PŘÍLOHA: ILUSTRAČNÍ PŘÍKLAD

Přílohou této Metodiky je Ilustrační příklad evidence zpracování osobních údajů v malé advokátní kanceláři.

Vzor č. 1: Ilustrační příklad evidence zpracování osobních údajů v malé advokátní kanceláři

#	Kategorie a charakteristiky zpracování osobních údajů	Příklady (fiktivní malá advokátní kancelář)
1.	Jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů [článek 30 odst. 1 písm. a) GDPR]:	Jméno a kontaktní údaje správce [●]; Jméno a kontaktní údaje případného společného správce [●]; Jméno a kontaktní údaje zástupce správce [●]; Jméno a kontaktní údaje pověřence pro ochranu osobních údajů [●].
2.	Identifikace příslušných zpracování osobních údajů [článek 30 odst. 1 písm. b) GDPR]:	Vedení spisů klientů Evidence zaměstnanců (+ výkazy práce)
3.	Proč (za jakým účelem) a na základě jakého právního titulu se osobní údaje v rámci zpracovávání zpracovávají [článek 30 odst. 1 písm. b) GDPR]?	**Klienti**: smlouva o poskytování právních služeb se subjekty údajů – plnění smlouvy, výkon právních povinností vyplývajících z předpisů upravujících výkon advokacie **Třetí osoby**: oprávněný zájem správce – plnění smlouvy s klientem; plnění právních povinností vyplývajících z předpisů upravujících výkon advokacie **Zaměstnanci**: pracovní smlouva, DPP, DPČ – plnění povinností vyplývajících ze smluv se zaměstnanci a ze zákoníku práce a zákona o zaměstnanosti
4.	Jaké osobní údaje jsou zpracovávány v rámci zpracování [článek 30 odst. 1 písm. c) GDPR]?	**Klienti**: jméno, adresa, datum narození, rodné číslo, rodinný stav a rodinná situace, finanční situace, bankovní účet, údaje o probíhajících/ukončených/hrozících soudních/exekučních/správních řízeních, údaje o případných trestních řízeních a trestních věcech **Třetí osoby**: jméno, adresa, datum narození, rodné číslo, rodinný stav a rodinná situace, finanční situace, bankovní účet, údaje o probíhajících/ukončených/hrozících soudních/exekučních/správních řízeních, údaje o případných trestních řízeních a trestních věcech **Zaměstnanci**: jméno, adresa, datum narození, bankovní účet, pracovní doba, rodinný stav, vzdělání, fotografie
5.	Z jakých zdrojů jsou osobní údaje získány [článek 30 odst. 1 písm. c) GDPR]?	**Klienti**: subjekty údajů, soudy, správní úřady **Třetí osoby**: klienti, subjekty údajů, soudy a soudní spisy, správní úřady, svědci, znalci, veřejné rejstříky, veřejně přístupné informace (např. internet) **Zaměstnanci**: subjekty údajů

#	Kategorie a charakteristiky zpracování osobních údajů	Příklady (fiktivní malá advokátní kancelář)
6.	Kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích:	- Účetní (společnost, samostatná) - IT firma udržující náš systém - Překladatelská agentura - Nezpřístupňujeme osobní údaje příjemcům ve třetích zemích ani v rámci mezinárodních organizací
7.	V jakém termínu a jak se osobní údaje likvidují [článek 30 odst. 1 písm. f) GDPR]?	Dle našeho archivního a skartačního řádu
8.	Jakým způsobem se osobní údaje aktualizují [článek 30 odst. 1 písm. g) GDPR]?	Informacemi od subjektů údajů, od třetích stran, případně pomocí veřejných zdrojů (internet, veřejné rejstříky…)
9.	Které listinné a elektronické evidence (spisovny, archivy, IT systémy, datová úložiště) provádějí zpracování [článek 30 odst. 1 písm. g) GDPR]?	Pro vedení klientské agendy používáme systém s názvem [●]. Dále pro účely přípravy pracovních návrhů dokumentů používáme sdílený disk advokátů a advokátních koncipientů; přístup na tento disk je chráněn heslem unikátním pro každého uživatele. Pro správu kanceláře používáme systém [●], který je napojený na účetní systém [●]. Všechny tyto tři systémy jsou standardní produkty pro advokátní kanceláře.
10.	Je prostředí AK pravidelně bezpečnostně testováno (zejm. IT systémy)? Interně nebo externími konzultanty? [článek 30 odst. 1 písm. g) GDPR].	Externími konzultanty 1x za 12 měsíců
11.	Jak je zajištěna bezpečnost předání dat při klientské komunikaci [článek 30 odst. 1 písm. g) GDPR]?	Přenos citlivých informací podléhá zaheslování
12.	Jak je zajištěna bezpečnost sdílení dat s externími subjekty? Mají všichni externí dodavatelé, zpracovávající osobní údaje, uzavřené smlouvy o zpracování osobních údajů, poskytující odpovídající záruky ochrany [článek 30 odst. 1 písm. g) ve spojení s článkem 28 GDPR]?	Ano. Smlouvy o zpracování osobních údajů máme uzavřeny s následujícími dodavateli: - Účetní (společnost, samostatná) - IT firma udržující náš systém - Překladatelská agentura
13.	Je zajištěna nevratná likvidace dat v rámci databázového systému [článek 30 odst. 1 písm. g) GDPR]?	Ano, data jsou likvidována, nejen deaktivována.
14.	Je k dispozici procedura k určení práv subjektů údajů a jejich výkon s ohledem na jejich data, která jsou zpracovávána v rámci zpracování?	Ano, umožňujeme každému podat žádost na našem webu, žádosti vyřizujeme v předepsaných lhůtách.
15.	Poskytují se oprávněným subjektům údajů předepsané informace, zejména o: - rozsahu a účelu zpracování, - způsobu zpracování osobních dat, - komu mohou být osobní údaje zpřístupněny?	Ano, informace poskytujeme následující formou: - na našem webu - ve smlouvě s klienty - v odpovědích na žádosti subjektů údajů

#	Kategorie a charakteristiky zpracování osobních údajů	Příklady (fiktivní malá advokátní kancelář)
16.	Zabraňují nasazené technické prostředky a uplatňovaná organizační opatření nahodilému anebo neoprávněnému přístupu k osobním údajům, jejich změně, zcizení, zneužití, zničení nebo ztrátě [článek 30 odst. 1 písm. g) GDPR]?	Ano, uplatňujeme zejména následující opatření: - K zpracovávaným spisům mají přístup pouze osoby, které se spisem pracují; - Spisy jsou zaheslované v počítači; spisy v listinné podobě se nacházejí v uzamykatelných skříních; - Přístup do kanceláří je zabezpečen kartou; - IT systém je standardní, vyzkoušený, používaný v řadě advokátních kanceláří. Přístup do IT systému je omezen podle nastavených manažerských rolí. - IT systém je pravidelně testován a udržován externím dodavatelem, se kterým jsme uzavřeli smlouvu o zpracování osobních údajů.
17.	Jsou zpracovávané osobní údaje přenášeny do zahraničí nebo jsou přístupné ze zahraničí [článek 30 odst. 1 písm. e) GDPR]?	Ano, výjimečně. Používáme vzorové smluvní doložky Evropské komise.
18.	Jsou pracovníci, mající přístup k osobním údajům v rámci zpracování osobních údajů, proškoleni? Mají tito pracovníci ve svých smlouvách sjednánu povinnost mlčenlivosti ve vztahu ke zpracovávaným osobním údajům [článek 30 odst. 1 písm. g) GDPR]?	Ano, proškolení probíhá jednak při nástupu do zaměstnání a dále jednou za 18 měsíců. Ano, pracovníci, kteří nejsou advokáty nebo advokátními koncipienty, mají v pracovních smlouvách závazek mlčenlivosti.