Vzor 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.). Je-li v AK vydán a naplňován, lze odkázat na příslušný interní předpis (např. spisový plán anebo směrnice o zpracování osobních údajů).

#	Kategorie a charakteristiky zpracování osobních údajů	Komentáře pro vyplnění
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.).
15.	Poskytují se oprávněným subjektům údajů předepsané informace, zejména o: - rozsahu a účelu zpracování, - způsobu zpracování osobních dat,	Uveďte, kde a jakou formou poskytujete předepsané informace pro subjekty údajů.

#	Kategorie a charakteristiky zpracování osobních údajů	Komentáře pro vyplnění
	- komu mohou být osobní údaje zpřístupněny?	
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.

Vzor: 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

#	Kategorie a charakteristiky zpracování osobních údajů	Příklady (fiktivní malá advokátní kancelář)
		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
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]?	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).

#	Kategorie a charakteristiky zpracování osobních údajů	Příklady (fiktivní malá advokátní kancelář)
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
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.