



## 28 NEJČASTĚJŠÍCH DOTAZŮ V SOUVISLOSTI S GDPR

### 1. Jak správně zabezpečit dokumenty, spisy, archivní složky v kanceláři? /stačí zamčená kancelář nebo se musí zamykat každá skříň?

Správce je povinen přijmou technická a organizační opatření s ohledem na povahu, rozsah a účely zpracování. Není přesně stanoveno, jaká opatření jsou adekvátní a jaká nedostatečná. Vše je třeba posoudit individuálně. Předně si musí složky vyhodnotit, jaké osobní údaje zpracovávají a v jaké formě. Pokud jsou uchovávány elektronicky, především připadá do úvahy užití šifrování elektronických souborů. Pokud mají složky spisy v papírové podobě, musí si sami zhodnotit případná rizika ztráty či odcizení zpracovávaných dat. Rozlišení uvádíme na dvou modelových případech:

**Příklad 1:** Kancelář složky je umístěna ve vícepodlažní budově. U vchodu do budovy je umístěn kamerový systém, příchody a odchody všech osob, vč. návštěv, jsou evidovány. Jednotlivé kanceláře složky (případně společná chodba) je přístupna na základě použití vstupní karty.

**Příklad 2:** Kancelář složky je umístěna v běžné budově bez stálé recepce. Do budovy je volný přístup všech osob. Kancelář (případně společná chodba) je přístupná bez omezení. V budově se nachází sídla dalších právnických osob. V tomto důsledku se v bezprostředním okolí kanceláře pohybuje větší množství neznámých a neevidovaných osob. Vstupní dveře do kanceláře jsou vybaveny průměrným snadno překonatelným zámekem.

Je evidentní, že v prvním případě je postačující prosté uzamknutí kanceláře, zatímco v případě druhém považujeme za vhodné uzamknout konkrétní skříň s osobními údaji, případně osobní údaje umístit do trezoru. Obecně, pokud to složkám nezpůsobí technické a finanční problémy, doporučujeme raději údaje zabezpečit v co nejširší možné míře.

### 2. Když je firma členem OHK automaticky souhlasí s rozesíláním mailingu nebo musí podepsat doložku o GDPR? Musí se i zpětně?

Obecně platí, že souhlas subjektu údajů musí být svobodný, konkrétní, informovaný a jednoznačný. Subjekt tak musí obdržet veškeré informace, vč. konkrétního účelu tak, aby subjekt údajů získal dostatečnou představu o tom, jak bude s jeho údaji nakládáno. V přihlášce člena tak doporučujeme přidat ustanovení, splňující tyto předpoklady. Poté bude možno automaticky rozesílat členům obchodní sdělení a emaily.

Co se týče platnosti souhlasů, které byly a ještě budou uděleny před účinností GDPR, ty budou platné i nadále pouze v případě, že způsob jejich udělení splňuje veškeré výše uvedené předpoklady! Jednotlivé složky si tak musí opět samy vyhodnotit, zda jimi užívané formulace použité při získání souhlasů jsou v souladu s GDPR či nikoliv. Obecně lze opět pouze doporučit vyžádat si nové souhlasy tak, aby vše plně odpovídalo GDPR.



3. **Můžeme na prezenční listiny seminářů, kterých se účastní i zájemci, kteří nejsou členy OHK, uvést větu, že v návaznosti na GDPR svým podpisem souhlasí s použitím jejich emailu k zasílání dalších návrhů na semináře a školení?**

Doporučujeme do přihlášek na konkrétní akce naformulovat souhlas se zpracováním osobních údajů tak, aby byl souladný s GDPR (k bližšímu odůvodnění viz otázka č. 2). U prezenčních listin nepovažujeme tuto formu za příliš vhodnou. Už jen z rýze praktického hlediska – v případě účasti více zájemců může mít prezenční listina více stran, v takovém případě by poučení a souhlas se zpracováním osobních údajů musel být na každé z nich, což je však vzhledem k rozsáhlosti prohlášení poměrně problematické.

4. **Stačí u mailového podpisu tato věta: Upozornění: V souvislosti se zákonem o ochraně osobních údajů sdělujeme, že se jedná o obchodní sdělení. Pokud nemáte zájem o rozesílku e-mailingu, odpovězte ne.**

Ano. Pokud složka disponuje osobními údaji, které se souhlasem subjektu získala v rámci své činnosti, případně souhlasem se zasíláním obchodních sdělení, pak postačí, aby informovala subjekt údajů o možnosti ukončit zasílání obchodních sdělení. Co se týče ukončení zasílání obchodních sdělení, případně odvolání souhlasu se zpracováním obecně, je třeba, aby tato možnost byla pro subjekt údajů snadno proveditelná!

5. **Když budeme oslovovat nové firmy (pozvání na semináře, akce,...), posílat na obecný e-mail (který neobsahuje jméno člověka)? Pak je to v pořádku?**

K zasílání obchodních sdělení je třeba souhlasu dotčeného subjektu (případně jiného právního titulu) i nadále. Nelze rozesílat náhodné emaily novým společnostem, jednalo by se o šíření nevyžádaných obchodních sdělení.

6. **V rámci úřadu využíváme 2 organizací – ohk cv a Hospodářskou a sociální radu Chomutovska (organizace pro obce, NNO,...) – kontakty se využívají oboustranně – jak to ošetřit, aby nás nikdo nenapadl?**

V daném případě se jedná dva samostatné subjekty (dva správce). Souhlas se zpracováním osobních údajů by měl být tedy pro každý subjekt samostatně, respektive v naformulovaném souhlasu explicitně uvést oba subjekty, všechny účely a veškeré informace tak, aby byly naplněny požadavky GDPR (k podrobnostem viz odpověď na otázku č. 2).

**Pozor!** Podle závěrů pracovní skupiny za situace, kdy v naformulovaném souhlasu bude jedním z účelů například zasílání obchodních sdělení a k tomu sdílení osobních údajů s dalšími subjekty (tj. například s další OHK), je třeba, aby měl subjekt údajů možnost souhlasit jen s některým účelem (tj. souhlas musí být rozdělen a subjektu musí být dána možnost volby).

Případně je možné, aby byli tzv. společní správci. Ovšem i v tomto případě je třeba subjekt údajů o těchto skutečnostech informovat.

7. **Fotografie – pro rekapitulaci: hromadné fotky (souhlas ne); fotky s předáváním cen – soutěže,...(souhlas ne); detailnější fotografie na skupinu, kde jsou vidět třeba přednášející / zástupci společností / prezentující se školy / exkurze do firem – organizuje ohk, škola vysílá děti za doprovodu pedagoga – pořízené fotografie – detailní, skupinové, apod... souhlas ano/ne?**



Pokud jsou jednotlivé osoby na fotografii jasně identifikovatelné, jedná se o osobní údaj, jehož zpracování (vč. zveřejnění) podléhá souhlasu subjektu údajů. V případě dětí mladších 16 let je k udělení souhlasu oprávněn zákonný zástupce.

**8. Posílání dokumentů ohk – mezi kanceláří a daň.poradkyní – e-mailem – je to ok? Je rozdíl dát info osobní povahy do těla e-mailu nebo jako příloha**

Správce je povinen přijmout dostatečná bezpečnostní opatření tak, aby nemohlo dojít ke zcizení, ztrátě či zneužití osobních údajů. Domníváme se, že zasílání těchto údajů prostým emailem tento požadavek nenaplní (email je přístupný prakticky pro kohokoliv, hesla bývají jednoduše prolomitelná a zabezpečení není v mnohých případech dostatečné).

Jako vhodnější považujeme způsob, kdy budou osobní údaje zasílány prostřednictvím datové schránky, či budou přístupny například na webových stránkách po přihlášení do zabezpečeného webového rozhraní, nebo uloženy na zabezpečeném vzdáleném úložišti, kam lze dát daňovému poradci přístup.

**9. Když pracujeme s nezaměstnanými (jejich osobní data) a nabízíme volná pracovní místa firmám či obráceně – jak uchovávat tato data??**

V takovém případě zpracováváte osobní údaje. Je třeba přijmout náležitá technická opatření tak, aby nemohlo dojít ke zcizení, poškození, či ztrátě těchto dat. Pokud jsou v elektronické formě, pak je možno data šifrovat, ukládat na zabezpečených úložištích, atp. Jestliže jsou data ve fyzické podobě (papírové formuláře), pak je možno je uložit do trezoru, uzamykatelného archivu, atp. (blíže viz odpověď na otázku č. 1).

**10. Archiv – obsahuje spoustu osobních dat – musíme je celé projít a data rušit nebo je tam můžeme nechat? Musí být v uzamykatelné kanceláři nebo skříni?**

Znovu procházet data není potřeba, pokud podle nich nebude postupováno – tj. pokud jsou v archivu umístěny souhlasy subjektů údajů, které mají být nadále využívány, pak je třeba tyto souhlasy projít a zkontrolovat, zda je jejich formulace v souladu s GDPR. Pokud si budou složky získávat nové souhlasy, pak procházení

**11. Pro zaměstnance na HPP bude souhlas se zpracováním os.údajů – jak detailně musí být tento dokument řešen? A vztahuje se i na DPČ, DPP...??**

Obecně musí být souhlas konkrétní, informovaný a svobodný. Zejména zde tedy musí být obsaženo, jaké údaje jsou zpracovávány, za jakým účelem a na jakou dobu. Tato povinnost se vztahuje na veškeré zpracovávané osobní údaje, tj. jak na zaměstnance v HPP, tak na zaměstnance, vykonávající práci na některou z dohod. Rozhodující totiž není právní vztah, nýbrž povaha zpracovávaných údajů.

Nicméně domníváme se, že v případě pracovněprávních vztahů je nejvhodnějším titulem nikoliv výslovný souhlas, nýbrž nezbytnost pro plnění pracovní smlouvy a nezbytnost pro plnění právních povinností, tj. samotný podpis pracovní smlouvy by měl být k údajům v rozsahu pracovní smlouvy postačující.

**12. Zpracování úč.dat externí firmou, IZ služby, apod.... – co vše musíme mít podepsáno, aby nemohli zneužít dat?**

Při uzavírání smluv s těmito externími subjekty je třeba pamatovat v jednotlivých ustanoveních na ochranu osobních údajů. Ve smlouvě je vhodné vymezit, jak budou data předávána, jak



s nimi má být nakládáno. Zároveň doporučujeme do smlouvy doplnit ustanovení, v němž externí subjekt výslovně prohlásí, že je schopen zajistit náležitou ochranu osobních údajů a že se zavazuje užívat osobní údaje pouze ke stanovenému účelu (tj. například pouze za účelem zpracování účetnictví/podání daňového přiznání, atp.).

**13. Úklidová služba – zajištění mlčenlivosti / ochrany dat – zajišťuje si firma sama nebo musíme my s ní něco podepsat?**

Ve smlouvě s úklidovou službou by měla být uvedena povinnost společnosti zajistit, aby všichni zaměstnanci, provádějící úklid v prostorách složky, měli podepsanou dohodu o mlčenlivosti. Rovněž je vhodné dát do smlouvy ustanovení, že společnost zajišťující úklidové služby bere na vědomí, že se v prostorách složky nachází osobní údaje a společnost je povinna zajistit, aby při realizaci předmětu smlouvy (tj. úklidu) nedošlo k jejich odcizení, zničení či ztrátě.

**14. Platí GDPR i pro ochranu údajů právnických osob?**

Nikoliv. Nařízení stanoví pravidla týkající se výhradně ochrany fyzických osob.

**15. Platí GDPR pro ochranu fyzických osob podnikajících jako OSVČ?**

Ano. Nařízení se obecně vztahuje na osobní údaje všech fyzických osob.

**16. Platí GDPR jako ochrana fyzických osob – občanů?**

Ano, viz otázky 15, 16.

**17. Vedeme evidenci právnických osob a OSVČ v uzamčených prostorách kanceláře Cechu na přihláškách v šanonech a na PC s heslem (outlook, seznam členů atd.). Prostory nejsou veřejně přístupné, hesla jsou osobní každého uživatele. Předpokládáme, že budeme mít podepsaný souhlas s evidencí osobních údajů od každého člena. Musí být zde speciální zabezpečení?**

Nařízení samo o sobě nestanovuje konkrétní pravidla pro zabezpečení dokumentů, obsahující osobní údaje. Není přesně stanoveno, jaká opatření jsou adekvátní a jaká nedostatečná. Vše je třeba posoudit individuálně. Pokud jsou přijata opatření, uvedená v dotazu, pak lze hodnotit toto zabezpečení jako maximální možné, jehož byl zpracovatel schopen.

**18. Mohou být počítače v kanceláři připojené k internetu?**

Ano. Pokud jsou v počítačích uchovávány osobní údaje, je třeba počítač náležitě zabezpečit proti případným internetovým útokům, či zničení/ztrátě. Tudíž například instalace antivirového softwaru, atp.

**19. Na webových stránkách máme seznam členů OSVČ, kde je jejich fotografie, adresa, email i telefon. Je to forma inzerce v rámci činnosti Cechu, aby si je mohli zákazníci najít a objednat. Samozřejmě budeme mít písemný souhlas. Může to být?**

Pokud subjekt údajů výslovně souhlasí s tím, aby jeho osobní údaje byly za tímto účelem zpracovávány formou zveřejnění na webových stránkách, pak lze uvedené údaje zveřejnit.

**20. V časopise vydáváme seznam našich členů s kontakty, zase je to součástí inzerce v rámci cechovní činnosti a budeme mít souhlas. Může to být? Vždy jsou to údaje z rejstříku Ares nebo Justice.**



Pokud subjekt údajů výslovně souhlasí s tím, aby jeho osobní údaje byly za tímto účelem zpracovávány formou zveřejnění na webových stránkách, pak lze uvedené údaje zveřejnit.

**21. Když nějakého člena vyloučíme pro nějaký závažný přečin, tak si samozřejmě tuto informaci uchováme, aby nám za rok zase nechtěl vstoupit znovu do Cechu a my nevěděli, co se stalo. Můžeme si uchovat tyto informace?**

Lze předpokládat, že o vyloučení člena rozhoduje příslušný orgán Cechu. Toto rozhodnutí, byť obsahuje osobní údaje (jméno, příjmení, atp.), je vydáváno na základě oprávněného zájmu Cechu a lze jej nadále uchovávat vč. těchto údajů. Ovšem i tyto údaje lze zpracovávat pouze o dobu nezbytně nutnou.

**22. To samé platí i při ukončení členství na vlastní žádost, případně odchodu do důchodu. Údaje si uchováme a posíláme například přání k narozeninám. Může to tak být, případně za jakých podmínek?**

Cechy zpracovávají osobní údaje svých členů na základě oprávněného zájmu, v některých případech na základě souhlasu (pořádání akcí, zasílání obchodních sdělení, atp.). Po skončení členství již nadále oprávněný zájem netrvá, nota bene ve vztahu k zasílání přání k narozeninám. Proto doporučujeme opatřit si od subjektu údajů souhlas s tím, aby jeho osobní údaje byly zpracovávány po skončení členství za účelem zasílání informací a sdělení.

**23. Faktury vystavené členům a jiným subjektům uchováme v účetnictví (šanoný) a předáváme je ke zpracování účetní firmě. Může to tak být nebo musí být nějaké speciální povolení či dobrozdání o uchování zabezpečení dat účetní firmy?**

Při uzavírání smluv s těmito externími subjekty je třeba pamatovat v jednotlivých ustanoveních na ochranu osobních údajů. Ve smlouvě je vhodné vymezit, jak budou data předávána, jak s nimi má být nakládáno. Zároveň doporučujeme do smlouvy doplnit ustanovení, v němž externí subjekt výslovně prohlásí, že je schopen zajistit náležitou ochranu osobních údajů a že se zavazuje užívat osobní údaje pouze ke stanovenému účelu (tj. například pouze za účelem zpracování účetnictví/podání daňového přiznání, atp.).

**24. Může chodit faktura emailovou poštou tak jako doposud?**

V případě, že je fakturační doklad zasílán fyzické osobě, doporučujeme si vyžádat souhlas subjektu údajů se zasíláním elektronického fakturačního dokladu prostým emailem. V případě, že se jedná o fakturaci mezi dvěma právními osobami, jejich údaje nepodléhají ochraně osobních údajů dle GDPR.

**25. Je faktura vůbec nějaký důležitý doklad, když je to pouze výzva k platbě?**

Řádně vystavený fakturační doklad, obsahující náležitosti daňového dokladu, má svůj význam především v rovině účetní a daňové. Z hlediska právního se nejedná ani o výzvu k platbě, nýbrž o prostou informaci odběrateli o tom, kolik stála předmětná služba a jak ji lze zaplatit. Pro případné soudní vymáhání je faktura sama o sobě naprosto nedostatečná, je třeba ji doložit dalšími listinami (uzavřenou smlouvou či objednávkou, nejlépe i dodacím listem s podpisem a razítkem odběratele, atp.).



- 26. Faktury vystavené členům a jiným subjektům uchováváme v účetnictví (šanoný) a předáváme je ke zpracování účetní firmě. Může to tak být nebo musí být nějaké speciální povolení či dobrozdání o uchování zabezpečení dat účetní firmy?**

V tomto případě je účetní firma zpracovatelem osobních údajů v rozsahu, který je dán úkoly, které pro nás plní. Faktury jsou účetní doklad vystavený na základě smluvního vztahu. Takže k jejich vystavování ani uchovávání není třeba žádné speciální oprávnění nebo souhlas. Účetní firma by měla být zavázána, že s osobními údaji bude nakládat v souladu s právními předpisy a bude předcházet jejich možnému zneužití (proveden taková opatření, aby ke zneužití dojít nemohlo).

- 27. Může chodit faktura emailovou poštou tak jako doposud?**

ANO

- 28. Je faktura vůbec nějaký důležitý doklad, když je to pouze výzva k platbě?**

Ano, faktura je účetní doklad a je pravdou, že ve skutečnosti jde o výzvu k platbě. Nicméně v účetnictví potřebujete takovéto doklady a faktura je proto dobrým nástrojem, i když samozřejmě lze i formou interních dokladů. V případě plátců DPH se náležitosti účetních a daňových dokladů řídí zákonem o DPH, faktura se musí vystavovat až u plateb od 10 000,- Kč, jinak lze zjednodušený daňový doklad. Záleží také na znění smlouvy, na základě které se platí. Takže v našem případě bych zůstala u faktury a dodržovala náležitosti dle zákona o DPH.