Náležitosti zpracovatelské smlouvy, kdy správce osobních údajů uzavírá smlouvu s dodavatelem za účelem zpracování osobních údajů

- Potřeba upřesnit vzájemné povinnosti vyplývá ze skutečnosti, že zpracovatel zpracovává osobní údaje jménem správce. **Správci musí** svým zpracovatelům **poskytnout pokyny týkající se každé činnosti jejich zpracování**. Tyto pokyny mohou zahrnovat přípustné a nepřijatelné nakládání s osobními údaji, podrobnější postupy, způsoby zabezpečení údajů atd. **Zpracovatel nesmí pokyny správce překročit**. Může však navrhnout prvky, které se v případě přijetí správcem stanou součástí daných pokynů.
- **Pokud zpracovatel** zpracovává údaje mimo **pokyny správce** nebo je **překračuje** a odpovídá to rozhodnutí určujícímu účely a prostředky zpracování, tím zpracovatel poruší své povinnosti, a v souladu s čl. 28 odst. 10 **bude** dokonce v souvislosti s tímto zpracováním **považován za správce**.
- **Pokyny** vydané správcem musí být **doloženy**. Pro tyto účely se doporučuje zahrnout do přílohy smlouvy nebo jiného právního aktu postup a šablonu pro udělování dalších pokynů. Pokyny mohou být případně poskytnuty v jakékoli písemné formě (např. e-mailem), jakož i v jakékoli jiné doložené podobě, pokud je možné vést záznamy o těchto pokynech. V každém případě, aby se zabránilo jakýmkoli obtížím při prokazování toho, že pokyny správce byly řádně doloženy, doporučuje se uchovávat tyto pokyny společně se smlouvou nebo jiným právním aktem.
- S odvoláním na čl. 28, odst. 3 musí zpracovatelská smlouva obligatorně obsahovat **předmět** zpracování, **dobu** trvání zpracování, **povahu** zpracování, **typ** osobních údajů **a kategorii osobních údajů**. Součástí smlouvy má být vymezen proces komunikace mezi správcem a zpracovatelem: kdo, komu, kdy, co a jak komunikuje.
- Povinnost zpracovatele zdržet se jakékoli činnosti zpracování, která není založena na pokynech správce, se vztahuje rovněž na **předávání** osobních údajů **do třetí země nebo mezinárodní organizaci**. Smlouva by měla specifikovat požadavky na předávání údajů do třetích zemí nebo mezinárodním organizacím s přihlédnutím k ustanovením kapitoly V GDPR (Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím). Doporučuje se, aby správce věnoval tomuto konkrétnímu bodu náležitou pozornost, zejména pokud zpracovatel přenese některé činnosti zpracování na jiné zpracovatele a pokud má zpracovatel divize nebo oddělení nacházející se ve třetích zemích. Pokud pokyny správce neumožňují předávat nebo sdělovat údaje do třetích zemí, nebude zpracovatel moci přidělit zpracování dílčímu zpracovateli ve třetí zemi, ani mu nebude povoleno, aby údaje zpracovával v jedné ze svých divizí mimo EU.
- Zpracovatel může zpracovávat jiné údaje, než jsou údaje v doložených pokynech správce, **pokud je zpracovatel povinen zpracovávat a/nebo předávat osobní údaje na základě práva EU nebo členského státu, které se na zpracovatele vztahuje**. Toto ustanovení dále ukazuje, že je důležité dohody o zpracování údajů pečlivě vyjednávat a vypracovávat, neboť například může být zapotřebí, aby si některá ze stran vyžádala právní poradenství ohledně existence takového právního požadavku. To je třeba provést včas, neboť zpracovatel má povinnost informovat správce o takovém požadavku před zahájením zpracování. Pouze v případě, že stejné právo (EU nebo členského státu) zakazuje zpracovateli informovat správce o „důležitých důvodech veřejného zájmu“, taková informační povinnost neexistuje. V každém případě může k jakémukoli předání nebo zpřístupnění dojít pouze v případě, že to povoluje unijní právo, a to i v souladu s článkem 48 GDPR (Předání či zveřejnění údajů nepovolená právem Unie). Zpracovatel musí zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti (čl. 28 odst. 3 písm. b) GDPR).
- Ve smlouvě musí být uvedeno, že zpracovatel musí zajistit, aby kdokoli, kdo umožní zpracování osobních údajů, byl zavázán **k zachování mlčenlivosti**. K tomu může dojít buď prostřednictvím zvláštního smluvního ujednání, nebo na základě již existujících zákonných závazků. Široký

pojem „osoby oprávněné zpracovávat osobní údaje“ zahrnuje zaměstnance a dočasné zaměstnance. Obecně řečeno, zpracovatel by měl **osobní údaje zpřístupnit pouze zaměstnancům, kteří je skutečně potřebují k plnění úkolů**, pro které správce zpracovatele najal. Závazek nebo povinnost zachovávat mlčenlivost musí být „vhodné“, tj. musí oprávněné osobě účinně zakázat zveřejnit jakékoli důvěrné informace bez povolení, a musí být dostatečně široké, aby zahrnovaly všechny osobní údaje zpracovávané jménem správce, jakož i podmínky, za nichž jsou osobní údaje zpracovávány.

- Zpracovatel musí přijmout všechna opatření požadovaná podle článku 32 (Zabezpečení zpracování) (čl. 28 odst. 3 písm. c) GDPR), který vyžaduje, **aby správce a zpracovatel provedli vhodná technická a organizační bezpečnostní opatření**. Ačkoli je tato povinnost již přímo uložena zpracovateli, jehož operace zpracování spadají do oblasti působnosti GDPR, povinnost přijmout veškerá opatření požadovaná podle článku 32 musí být zohledněna ve smlouvě o činnostech zpracování svěřených správcem.
- Jak bylo uvedeno výše, **smlouva o zpracování by neměla pouze přeformulovávat ustanovení GDPR**. Smlouva musí obsahovat nebo odkazovat na informace o bezpečnostních opatřeních, která mají být přijata, **povinnost zpracovatele získat souhlas správce před provedením změn** a pravidelný přezkum bezpečnostních opatření s cílem zajistit jejich vhodnost s ohledem na rizika, která se mohou časem vyvinout. Míra podrobnosti informací o bezpečnostních opatřeních, jež mají být součástí smlouvy, musí být taková, aby správci umožnila posoudit vhodnost opatření podle čl. 32 odst. 1 GDPR. Popis je navíc nezbytný také proto, aby správce mohl plnit svou povinnost odpovědnosti podle čl. 5 odst. 2 (správce musí doložit odpovědnost za dodržování zásad zpracování osobních údajů) a článku 24 GDPR (obecné povinnosti správce), pokud jde o bezpečnostní opatření uložená zpracovateli. Odpovídající povinnost zpracovatele pomáhat správci a zpřístupňovat veškeré informace nezbytné k prokázání souladu lze vyvodit z čl. 28 odst. 3 písm. f) a h) GDPR.
- **Úroveň pokynů**, které správce zpracovateli poskytne, pokud jde o opatření, která mají být provedena, bude záviset **na konkrétních okolnostech**. V některých případech může správce poskytnout jasný a podrobný popis bezpečnostních opatření, která mají být provedena. V ostatních případech může správce popsat minimální bezpečnostní cíle, jichž má být dosaženo, a zároveň požádat zpracovatele, aby navrhl provedení konkrétních bezpečnostních opatření. Správce musí zpracovateli v každém případě poskytnout popis činností zpracování a bezpečnostních cílů (na základě posouzení rizik provedeného správcem) a schválit opatření navržená zpracovatelem. To by mohla obsahovat příloha smlouvy. Správce vykonává svou rozhodovací pravomoc ohledně hlavních rysů bezpečnostních opatření, ať již výslovným uvedením opatření, nebo schválením opatření navržených zpracovatelem.

Mgr. Ing. Josef Svoboda, Ph.D., pověřenec GDPR ČVUT v Praze
Vydáno 2024
Zdroj: Pokyny 07/2020 k pojmům správce a zpracovatele v GDPR, verze 2.0, přijato organizací Data Protection Supervisor (EDPS)- Coordinated Supervision Committee dne 7. července 2021 (www.edpb.europa.eu/edpb_cs)