

**Příloha č. 5 – Principy smlouvy se Zpracovatelem.**

Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci. Smlouva má povinně písemnou formu, vč. elektronické formy.

Konkrétní parametry smlouvy o zpracování osobních údajů, které je nutné do smlouvy promítnout:

Článek GDPR	Povinnost správce/zpracovatele	Dopad do smlouvy
čl. 28 odst. 9	Požadavek na písemnou formu, vč. elektronické formy.	Smlouva musí mít písemnou formu. Zásadně a bezvýjimečně.
čl. 28 odst. 1	Správce může jako zpracovatele zapojit pouze takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.	Je nutné explicitní prohlášení zpracovatele, že zaručí zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.
čl. 28 odst. 2, věta první	Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce.	V případě, že je předpoklad „řetězení zpracovatelů“, je nutné explicitně uvést do ustanovení smlouvy ve variantě konkrétního nebo obecného písemného povolení ze strany správce
čl. 28 odst. 2, věta druhá	V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.	Je-li ve smlouvě uvedeno obecné povolení ze strany správce, že je umožněno „řetězení zpracovatelů“, je nutné zakotvit ve smlouvě proceduru pro přijetí nových zpracovatelů nebo jejich nahrazení a pro reakci správce
čl. 28 odst. 3, věta první	Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce.	V současnosti dle § 6 ZOOÚ. Smlouva musí obsahovat taxativně uvedené náležitosti: -závazky zpracovatele vůči správci, -předmět a doba trvání zpracování, -povaha a účel zpracování, -typ osobních údajů, -kategorie subjektu údajů, -povinnosti a práva správce.
čl. 28 odst. 3, věta druhá	povinnosti zpracovatele	Je nutné ve smlouvě uvést všechny dále uvedené povinnosti zpracovatele.
čl. 28 odst. 3, písm. a)	zpracovatel je oprávněn zpracovávat osobní údaje na základě doložených pokynů správce, vč. předání do třetích zemí a mezinárodním organizacím	Všechny pokyny musí být výslovně uvedeny ve smlouvě s výjimkou případů, kdy je mi to uloženo právem EU nebo členského státu, které se na správce vztahuje. V tomto případě jde pouze o informování správce ze strany zpracovatele (pokud to není zakázáno v důležitém veřejném zájmu).
čl. 28 odst. 3, písm. b)	osoby oprávněné zpracovávat musí být zavázány k mlčenlivosti nebo musí být zavázány k mlčenlivosti zákonnou povinností	Ve smlouvě specifikovat jednu z možností, tedy buď, že se zpracovatel zavazuje zajistit, aby všechny osoby, které zpracovávají osobní údaje, byly vázány mlčenlivostí nebo uvést konkrétně právní předpis, na základě kterého už tyto osoby vázány k mlčenlivosti jsou.
čl. 28 odst. 3, písm. c)	zpracovatel se zaváže, že přijme všechna opatření k zabezpečení zpracování	Ve smlouvě musí být specifikován závazek zpracovatele přijmout všechna opatření dle GDPR (čl. 32) a dále uvedena ona opatření.
čl. 32	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.	S přihlédnutím k <ul style="list-style-type: none"> <li>• stavu techniky,</li> <li>• nákladům na provedení,</li> <li>• povaze zpracování,</li> <li>• rozsahu zpracování,</li> <li>• kontextu zpracování a</li> <li>• účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, tj. tato opatření musí kopírovat analýzu rizik v případě</li> </ul>

		uzavíraných smluvních vztahů. Konkrétně – GDPR zná DEMONSTRATIVNÍ VÝČET, což znamená, že se jedná pouze o příklady, opatření mohou být i jiná, ALE správce/zpracovatel musí prokazovat, proč použil zrovna tato opatření. a) pseudonymizace a šifrování osobních údajů; b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
čl. 28 odst., 3 písm. d) čl. 28 odst. 4 čl. 28 odst. 2	zpracovatel dodržuje pravidla „řetězení“ zpracovatelů	Ve smlouvě je uveden závazek zpracovatele, že v případě, že zapojí do zpracování dalšího zpracovatele, zaváže ho smlouvou ke stejným povinnostem, které má ve vztahu ke správci, zejména k poskytnutí dostatečných záruk k zavedení vhodných technických a organizačních opatření k zajištění souladu podmínek zpracování osobních údajů s GDPR. Zároveň by měla ve smlouvě být uvedena ta skutečnost (s odkazem na čl. 28 odst. 4), že v případě, pokud tuto povinnost dále zapojený zpracovatel nesplní – odpovídá pak za všechny povinnosti ve vztahu ke správci on.
čl. 28 odst. 3, písm. e)	zpracovatel zohledňuje povahu zpracování a je nápomocen správci i při vyřizování žádostí subjektu údajů	Ve smlouvě stanoven závazek zpracovatele být nápomocen zejména tím, že přijme vhodná technická a organizační opatření
čl. 28 odst. 3, písm. f) čl. 32 až 36	zpracovatel je nápomocen správci v plnění povinností dle čl. 32 až 36	Ve smlouvě jsou konkrétně vyjmenované povinnosti správce, při kterých je zpracovatel nápomocen: -zabezpečení zpracování (čl. 32), -ohlašování případů porušení zabezpečení osobních údajů dozоровému úřadu (čl. 33), -oznamování případů porušení zabezpečení osobních údajů subjektu údajů (čl. 34), -posouzení vlivu na ochranu osobních údajů (čl. 35), -předchozí konzultace (čl. 36).
čl. 28 odst. 3, písm. g)	Na pokyn správce zpracovatel osobní údaje vymaže nebo po ukončení zpracování vrátí správce a všechny osobní údaje vymaže (s výjimkou případů, kdy je stanoveno právem EU nebo členského státu)	Ve smlouvě musí být upraven celý životní cyklus osobních údajů.
čl. 28 odst. 3 písm. h)	Povinnost zpracovatele doložit správci to, že jsou splněny všechny povinnosti dle čl. 28 a umožnit audity, vč. inspekci prováděných správcem či jím pověřenou osobou a poskytne součinnost u těchto auditů.	Explicitně tuto novou povinnost uvést ve smlouvě. Zároveň s povinností zpracovatele informovat neprodleně správce v případě, že jeho pokyn porušuje GDPR nebo jiný právní předpis.
čl. 26	Povinnosti společných správců	V případě společných správců mezi sebou transparentním ujednáním tuto vymezí: -své podíly na odpovědnosti za plnění povinností podle GDPR, zejména pokud jde o výkon práv subjektu údajů, -své povinnosti poskytovat informace uvedené v člancích 13 a 14, pokud tuto odpovědnost správců nestanoví právo Unie nebo členského státu, které se na správce vztahuje. V ujednání může být určeno kontaktní místo pro subjekty údajů. Dále ujednání zohlední úlohy společných správců a jejich vztahy vůči subjektům údajů. Subjekt údajů musí být o podstatných prvcích ujednání informován. POZOR: Bez ohledu na podmínky ujednání může subjekt údajů vykonávat svá práva podle tohoto nařízení u každého ze správců;