Náležitosti zpracovatelské smlouvy

Požadavky na zpracovatelskou smlouvu jsou přesně formulovány v **Obecném nařízení o ochraně osobních údajů**, konkrétně v jeho **článku 28**.

Článek 28 GDPR - Zpracovatel

1. Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.
=> důvod: 81, ,

2. Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. 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.
=> důvod: 171

3. 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. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:
=> důvod: 79, 81,

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

c) přijme všechna opatření požadovaná podle Článek 32;

d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;

e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;

f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů; ,

h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

Pokud jde o první pododstavec písm. h), informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů.

4. Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel. , ,

5. Jedním z prvků, jimiž lze doložit dostatečné záruky podle odstavců 1 a 4 tohoto článku, je skutečnost, že zpracovatel dodržuje schválený kodex chování uvedených v Článek 40 nebo schválený mechanismus pro vydávání osvědčení uvedený v Článek 42. ,

6. Aniž jsou dotčeny individuální smlouvy mezi správcem a zpracovatelem, mohou být smlouvy nebo jiné právní akty podle odstavců 3 a 4 tohoto článku založeny zcela nebo částečně na standardních smluvních doložkách podle odstavců 7 a 8 tohoto článku, mimo jiné i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli podle článků 42 a 43.

7. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky stanovit Komise přezkumným postupem podle čl. 93 odst. 2.

8. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky přijmout dozorový úřad v souladu s mechanismem jednotnosti uvedeným v Článek 63.

9. Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu.

10. Aniž jsou dotčeny články 82, 83 a 84, pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce. (vztahují se na něj přísnější pravidla)
=> Článek: 82,

Podle výše uvedeného článku 28 se zpracování zpracovatelem 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.

Smlouva musí také mimo jiné obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. Pokud tuto smlouvu správce osobních údajů nemá, dopouští se již dnes přestupku a stejně na to pohlíží i Obecné nařízení o ochraně osobních údajů.

Tyto informace jsou jakousi ochranou a zaručují, že zpracovatel:

- *zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně otázek předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;*
- *zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;*
- *přijme všechna opatření požadovaná podle článku 32*;

Článek 32 GDPR - Zabezpečení zpracování

1. 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, případně včetně:
=> Článek: 24, ,

a) pseudonymizace a šifrování osobních údajů;
=> Článek: 4,

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.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
=> důvod: 75, ,

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v Článek 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v Článek 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.
=> Článek: 29

Zpracovatel dále zejména:

- *dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;*
- *zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v GDPR kapitole III;*
- *je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;*
- *v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;*
- *poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.*

Zpracovatelská smlouva nebo jiný právní akt musí být podle nařízení GDPR vyhotoveny písemně, nikoli však nutně na papíře. Počítá se i elektronická forma dokumentu. Dále není nutné, aby se jednalo o samostatnou smlouvu. Požadované náležitosti je možné zakomponovat i do jiné smlouvy, kterou správce se zpracovatelem v rámci obchodního či jiného vztahu uzavírá, nebo je řešit dodatkem k původní smlouvě.

Taková smlouva je důležitou ochranou před problémy, které v souvislosti s ochranou osobních údajů hrozí každému správci.

Správce má zákonnou **povinnost využít** ke zpracování těchto dat **pouze ty zpracovatele**, kteří **poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření** tak, aby dané zpracování **splňovalo požadavky nařízení GDPR** a byla zajištěna **ochrana práv subjektu údajů**.

Malá rekapitulace

Správci a zpracovatelé mají odlišné povinnosti. **Pro správce platí přísnější podmínky pro zacházení s osobními údaji**. Zodpovídá za to, že zpracovatelé, kteří pro něj pracují, mají všechno v pořádku a osobní údaje jsou u nich v naprostém bezpečí, správně nastavená smlouva chrání obě strany.

Na co ve zpracovatelské smlouvě určitě nezapomenout?

Co a na jak dlouho

Ve smlouvě by mělo být stanoveno, že správce a zpracovatel spolupracují na základě smluvního vztahu, při kterém dochází k předávání osobních údajů. Ideálně uveďte, že **správce určuje účel zpracování osobních údajů**, poskytuje na jejich zpracování finanční prostředky a zpracovatel pro správce předané osobní údaje zpracovává v souladu s právními předpisy.

Vyjmenujte ve smlouvě kategorie osobních údajů, které si mezi sebou předáváte, a způsob, jakým k tomu dochází. Co to znamená v praxi? Neposílejte si mezi sebou osobní údaje v nezabezpečených formátech jako přílohu e-mailu a už vůbec ne v těle mailu.

Doba zpracování by měla být součástí dokumentace (řídíte se vždy účelem zpracování), kterou správce zpracovateli poskytuje spolu s osobními údaji. Myslete ve smlouvě také na to, co se s osobními údaji stane, pokud mezi sebou ukončíte spolupráci. Např. předání veškerých údajů správci. Jako správce si pak po uplynutí stanovené doby ověřte, že zpracovatel vám skutečně dané údaje předal a sám je odstranil, a to i ze všech záloh.

Proč a na co

Pokuste se ve smlouvě co nejpodrobněji popsat, k jakému účelu osobní údaje potřebujete. Myslete ale na to, že osobní údaje je nutné zpracovávat v co nejomezenější míře omezení účelem a pouze k danému účelu. Pokud se jedná o zpracování na základě souhlasu subjektu údajů, jakékoli dodatečné změny zpracování jsou bez souhlasu subjektu údajů neoprávněné. Jinými slovy - **účely vymezené zpracovatelskou smlouvou musí korespondovat se zněním souhlasu, který subjekty údajů poskytly**.

Co musíte a co můžete

Tato část smlouvy je klíčová, GDPR jí přikládá vysokou důležitost, a rozhodně by nemělo zůstat jen u prázdných vět na papíře bez faktického dodržování.

Stanovte si, že se zpracovatel zavazuje přijmout opatření potřebná k bezpečnému zpracovávání osobních údajů – jak vyhodnotíte v rámci předběžné analýzy rizikovost zpracování, je pouze na vašem uvážení. Určitě ale **nezapomeňte na povinnosti zpracovatele ohledně zabezpečení přístupu k datům, zamezení předání osobních údajů třetím osobám**. Zvažte také, zda přístup k datům neomezíte s ohledem na snížení rizika jen na konkrétní určité osoby. K elektronickým přenosů dat používejte vždy maximální zabezpečení, případně šifrování a pouze ověřený software.

Samostatnou kapitolou je pak **předávání dat dalším zpracovatelům**. **K tomu nikdy nesmí docházet bez souhlasu správce**. Pokud by to mělo nastat, nezapomeňte o tom informovat subjekty údajů, jejichž data předáváte a být připraveni na to, že můžou vznést námitku proti takovému zpracování.

Ve smlouvě explicitně uveďte také to, že **zpracovatel bude zpracovávat osobní údaje pouze v takové podobě, v jaké je od správce obdržel**, pouze za účelem, za kterým mu byly svěřeny, a pouze po dobu stanovenou účelem.

Nikdy nesdružujte seznamy a databáze osobních údajů, které byly získány k rozdílným účelům.
I toto si stanovte ve smlouvě.

Neměla by v ní chybět ani **povinnost zpracovatele opravit či smazat osobní údaje podle pokynů správce**.

Nezapomeňte také na zásadní **závazek mlčenlivosti zpracovatele**, vč. zaměstnanců nebo případných externích spolupracovníků. Ten musí trvat i po skončení zpracování nebo ukončení smluvního vztahu. Musí jednoznačně zavázat všechny zúčastněné osoby zpracovatele.

Co když dojde k porušení povinností. I na to musíte ve smlouvě myslet. **Nastavte smluvně konkrétní odpovědnosti správce i zpracovatele** a **myslete** při tom opět i na **zaměstnance a externí pracovníky**, na možnost případných sankcí od dozorového úřadu a samozřejmě na případnou úhradu způsobené škody. Dle míry možných rizik výšky případné škody, můžete zavázat zpracovatele k povinnosti mít uzavřenou pojistku na škody způsobené porušením zpracovatelské smlouvy.

Jak by měla smlouva vypadat?

Že musí být písemná, je jasné. Zda bude v listinné nebo pouze elektronické podobě je jen na vás, stejně tak, jestli zrušíte původní a uzavřete novou nebo to vyřešíte pomocí dodatku k původní smlouvě.

A jedna důležitá rada na závěr

Primární odpovědnost je vždy na správci. Co nebude ve smlouvě uvedeno, jako by neexistovalo. Než smlouvu podepíšete, důkladně si ji projděte.