39.19. Zpracovatel

http://www.guard7.cz/gdpr/zpracovatel

Zpracovatel Podle článku 28 nařízení Evropského parlamentu a raduy EU 2016/679 – GDPR

Zpracovatel je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

Správce by měl využít pouze takového zpracovatele, který s ohledem na povahu, kontext, kategorii osobních údajů a jejich možností, poskytuje dostatečné záruky vhodných technických a organizačních opatření, tak aby zpracování osobních údajů prostřednictvím zpracovatele splňovalo požadavky GDPR a byla zajištěna ochrana práv subjektu údajů. Za tím účelem musí být mezi správcem a zpracovatelem uzavřena písemná smlouva.

 *Náležitosti smlouvy mezi správcem a zpracovatelem*

Není nutné, aby se jednalo o samostatnou smlouvu, lze požadované náležitosti zakomponovat i do jiné smlouvy, kterou správce se zpracovatelem uzavírá v rámci např. obchodního či jiného vztahu. Správce se přizváním zpracovatele nezbavuje odpovědnosti za zpracování osobních údajů.
Pokud zpracovatel zapojí dalšího zpracovatele, je nutné, aby správce k tomuto dal písemné svolení. Svolení může být dáno k dalšímu konkrétnímu zpracovateli, nebo může být dáno obecné svolení, v takovém případě však zpracovatel musí správce informovat o veškerých přijetích dalších zpracovatelů nebo jejich nahrazení. Účelem tak je, aby správce, který za zpracování osobních údajů primárně odpovídá, věděl, které subjekty pro něj osobní údaje zpracovávají.

Typickým zpracovatelem je externí účetní nebo marketingová firma, IT firma s přímým a popřípadě dálkovým přístupem k datům.

Související legislativa

Zákon č. 101/2000 Sb., o ochraně osobních údajů.
Zákon č. 89/2012 Sb., občanský zákoník.
Zákon č. 127/2005 Sb. ,o elektronických komunikacích.
Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.
Nařízení GDPR

Článek 28
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.

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.

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:

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 článku 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 článku 40 nebo schválený mechanismus pro vydávání osvědčení uvedený v článku 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 článku 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.

Článek 29
Zpracování z pověření správce nebo zpracovatele

Zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu.

Zpracování osobních údajů správce zpracovatelem se řídí smlouvou nebo jiným právním aktem, které zavazují zpracovatele vůči správci a v nichž je stanoven:

1. předmět zpracování,
2. doba trvání zpracování,
3. povaha a účel zpracování,
4. typ osobních údajů,
5. kategorie subjektů údajů,
6. povinnosti a práva správce,
7. povinnosti a práva zpracovatele.

Tato smlouva nebo jiný právní akt stanoví, že zpracovatel:

1. 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;
2. zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
3. přijme všechna opatření požadovaná podle článku 32 tj.

- 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:

    - pseudonymizace a šifrování osobních údajů;
    - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
    - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
    - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

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

1. dodržuje podmínky pro zapojení dalšího zpracovatele,
2. 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, je správci nápomocen při zajišťování souladu s povinnostmi při zabezpečení osobních údajů a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici,
3. 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,
4. 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,
5. zpracovatel informuje neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje nařízení GDPR nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů,
6. 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 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,

7. jedním z prvků, jimiž lze doložit dostatečné záruky je skutečnost, že zpracovatel dodržuje schválený kodex chování nebo schválený mechanismus pro vydávání osvědčení,
8. aniž jsou dotčeny individuální smlouvy mezi správcem a zpracovatelem, mohou být smlouvy nebo jiné právní akty založeny zcela nebo částečně na standardních smluvních doložkách, mimo jiné i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli,
9. pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky stanovit Komise přezkumným postupem,
10. pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky přijmout dozorový úřad v souladu s mechanismem jednotnosti uvedeným v článku 63,
11. smlouva nebo jiný právní akt podle musí být vyhotoveny písemně, v to počítaje i elektronickou formu,
12. pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.