Kodexy chování

metodická příručka verze 1.0

Úvod

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále též obecné nařízení o ochraně osobních údajů nebo také jen nařízení) zdůrazňuje větší odpovědnost správců a zpracovatelů za jimi prováděná zpracování osobních údajů.

Kodexy chování podle obecného nařízení poskytují příležitost subjektům v daném odvětví dohodnout se společně na konkrétních a praktických pravidlech při zpracování osobních údajů v daném odvětví, která budou splňovat požadavky nařízení. **Cílem tohoto materiálu je přiblížit veřejnosti problematiku kodexů chování, vysvětlit jejich podstatu, naznačit základní pravidla a doporučit praktické postupy. Aby byl materiál kompletní, obsahuje i stručný popis mechanismu monitorování kodexu, bez kterého by kodex chování nebyl životaschopným nástrojem ochrany osobních údajů.**

Kodex chování jako dobrovolný systém samoregulace

Kodex chování je samoregulačním nástrojem, který by měl zohledňovat specifika různých odvětví. Konečným cílem konkrétního kodexu by v žádném případě nemělo být pouhé opisování jednotlivých článků nařízení, ale řešení nejasností a specifik, které vznikají při zpracování osobních údajů v rámci daného odvětví (pojišťovnictví, bankovnictví, zdravotnictví, cestovní ruch apod.). Jak je uvedeno v recitálu (98) obecného nařízení o ochraně osobních údajů, kodexy by měly zejména upřesňovat povinnosti správců a zpracovatelů s přihlédnutím k riziku, které ze zpracování pravděpodobně vyplyne pro práva a svobody fyzických osob.

Správce nebo zpracovatel může prokázat soulad operací zpracování osobních údajů s nařízením sám, a to předložením odpovídající dokumentace například v rámci kontroly prováděné Úřadem pro ochranu osobních údajů nebo při uzavírání zpracovatelské smlouvy. U některých správců tento postup zcela postačuje a není třeba využít jiných nástrojů. Nicméně nařízení rovněž zavádí v zásadě nové, nepovinné nástroje, umožňující výše uvedeným subjektům zajistit nezávislé a nestranné vyhodnocení a prokázání souladu operací zpracování s tímto nařízením. Jedním z takových nástrojů je závazek k dodržování kodexu chování přijatý správcem nebo zpracovatelem.[1]

[1] článek 40 a 41 nařízení 2016/679

Kodex chování je tedy stručně řečeno předem připravený text (upravující zásady a požadavky na zpracování osobních údajů) opatřený závazkem subjektu (správce nebo zpracovatele) k dodržování v kodexu popsaných postupů. Závazek zahrnuje rovněž zajištění monitorování dodržování kodexu (viz dále v textu). Vzhledem k tomu, že příprava kodexu chování bude poměrně náročnou činností, mělo by dojít k jeho vypracování výlučně pro skupiny obdobných operací zpracování osobních údajů prováděnými správci nebo zpracovateli s obdobným charakterem činnosti (například v rámci provozování internetových obchodů, cestovních kanceláří, lékařských ordinací, zpracování účetnictví apod.).

Kodex chování a role Evropského sboru

Významná úloha při uplatňování obecného nařízení v oblasti kodexů chování připadá Evropskému sboru pro ochranu osobních údajů (navazujícímu na dřívější WP29, dále jen „Sbor“). Jeho role spočívá v přípravě metodických návodů (viz např. Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679) a také v zajištění jednotného výkladu obecného nařízení o ochraně osobních údajů (schvalování akreditačních požadavků a některých kodexů chování). Z toho důvodu bude nutné vyčkat na dokončení výše uvedených návodů a až poté začít zakládat celý systém přípravy a monitorování kodexů. Sladění s připravovanými vodítky je nezbytně nutné, aby nedocházelo k vytváření návrhů, které nemohou být schváleny, a k nežádoucím změnám v podmínkách akreditací subjektů pro monitorování kodexů a struktuře kodexů chování. **Nicméně narůstající zájem z různých odvětví o kodexy i předčasné zasílání návrhů kodexů chování Úřadu pro ochranu osobních údajů k posouzení, ze kterých lze vypozorovat neporozumění podstatě tohoto samoregulačního nástroje, vede Úřad k vydání tohoto metodického materiálu.**

Základní postupy při zpracování kodexů

Níže uvedené postupy by měly případným zájemcům o vypracování kodexu pomoci se zorientovat v dané problematice a uvědomit si všechny souvislosti, které je nutné brát vždy v úvahu předtím, než se zájemce rozhodne řešit soulad s nařízením prostřednictvím kodexu.

1) Kodex chování spravuje určený subjekt (asociace, aliance, sdružení apod.), který se zaváže i k zajištění jeho aktualizace ve vztahu k vývoji legislativy, změnám postupů správců nebo zpracovatelů, případně i k vývoji informačních technologií.

2) Skupina správců nebo zpracovatelů v rámci konkrétního odvětví by měla mít jen jeden kodex (nelze mít několik rozdílných kodexů chování pro zpracování osobních údajů obdobného charakteru například provozování internetových obchodů, pojišťovnictví apod.).

3) Kodexy chování nejsou určeny pro jednotlivé správce nebo zpracovatele, nebo početně omezené skupiny správců nebo zpracovatelů (zejména z důvodu zajištění monitorování

kodexu chování). K zajištění souladu s obecným nařízením o ochraně osobních údajů v tomto případě slouží jiné nástroje, jako je bezpečnostní dokumentace, metodiky, směrnice, ale i certifikace apod.

4) Teprve ve chvíli, kdy je kodex chování schválen dozorovým úřadem nebo Sborem a současně jsou Sborem schváleny rovněž akreditační požadavky, může se ke kodexu přihlásit příslušný správce nebo zpracovatel.

5) Závazek správce nebo zpracovatele k dodržování kodexu chování je **dobrovolný**. Zejména v případě zpracovatele/dodavatele IT řešení a technologií (pokud je v pozici zpracovatele) je na místě závazek řádně zvážit, neboť by se podpisem různých kodexů chování mohl dostat do obtížně řešitelných problémů, protože některé povinnosti plynoucí z různých kodexů by mohly být v rozporu.

6) Zveřejnění závazku k dodržování kodexu chování je věcí správce nebo zpracovatele, který jej přijal.

7) Správce nebo zpracovatel se podpisem kodexu zavazuje k jeho dodržování, zajištění monitorování kodexu chování (prostřednictvím akreditovaného subjektu oprávněného k monitorování daného kodexu, a to včetně poskytnutí případné součinnosti tomuto akreditovanému subjektu, jako je poskytnutí veškerých podkladů, oznámení veškerých informací/změn, které mohou ovlivnit způsobilost správce a zpracovatele dodržet kodex chování).

8) Přihlášení se ke kodexu nemůže být podmiňováno plněním dalších povinností (mimo povinnosti uvedené v bodě 8) nebo odebíráním služeb nebo výrobků ve vztahu k subjektu, který spravuje kodex chování. Nelze například podmiňovat přistoupení ke kodexu nákupem zboží nebo zajištěním dalších služeb apod.

9) Kodex konkretizuje požadavky týkající se zpracování a ochrany osobních údajů, to znamená, že rozpracovává jednotlivá ustanovení obecného nařízení o ochraně osobních údajů tak, aby byla obdobná zpracování osobních údajů prováděná určitým typem správců v souladu s tímto nařízením.

10) Kodex nemá obsahovat pouze přepis ustanovení obecného nařízení o ochraně osobních údajů (takový kodex je zbytečný, protože ustanovení obecného nařízení o ochraně osobních údajů jsou přímo účinná). Uvedené neplatí pouze pro ta ustanovení obecného nařízení, která jsou podmíněná/fakultativní (mohou nebo nemusí platit).

11) Ustanovení kodexu chování musí být natolik konkrétní, aby umožňovala správci nebo zpracovateli jejich jednoznačnou implementaci a subjektu monitorujícímu kodex chování ověření jejich plnění.

12) Ustanovení kodexu chování mohou být jednak pozitivní (co správce nebo zpracovatel dělat musí), jednak negativní (co správce nebo zpracovatel dělat nesmí).

13) Nedílnou součástí každého ustanovení kodexu je komentář, který popisuje přidanou hodnotu každého ustanovení kodexu vůči obecnému nařízení o ochraně osobních údajů, případně zdůvodňuje, jak předkladatel došel k závěru uvedenému v ustanovení kodexu (například výběru technických a organizačních opatření by měla předcházet odpovídající analýza).

14) V jednotlivých ustanoveních je vhodné řešit nejen věcnou, ale i procesní stránku činností při zpracování osobních údajů.

15) Kodex nemůže anulovat povinnosti dotčených subjektů vyplývající z obecného nařízení o ochraně osobních údajů.

16) K zajištění monitorování kodexu chování[2] se může u Úřadu pro ochranu osobních údajů přihlásit jakýkoliv subjekt splňující Úřadem zveřejněné akreditační požadavky. Vyhodnocení plnění akreditačních požadavků zajišťuje Úřad pro ochranu osobních údajů. Akreditační požadavky musí být nejdříve zaslány Sboru ke schválení.[3]

Doporučený postup pro zpracovatele kodexu

Vzhledem k tomu, že kodex je určen pro stejnou skupinu správců nebo zpracovatelů, bude zhotoven zpravidla v rámci sdružení těchto správců nebo zpracovatelů nebo subjektem zastupujícím takovou skupinu správců nebo zpracovatelů nebo subjektem pracujícím na základě smlouvy. **Úřad pro ochranu osobních údajů kodexy nezpracovává, ve fázi přípravy kodexu pouze poskytuje nezbytné konzultace a následně předložený kodex posoudí, vydá stanovisko o tom, zda je návrh kodexu v souladu s nařízením a schválí jej.** Zpracování kodexu bude poměrně časově náročnou záležitostí, vyžadující odborné znalosti a někdy i vyšší finanční prostředky. Návrh kodexu nebo návrh úpravy kodexu musí být následně předložen Úřadu pro ochranu osobních údajů, a to požadovaným postupem a v požadované struktuře (ve smyslu pokrytí všech požadavků kladených na správce nebo zpracovatele obecným nařízením o ochraně osobních údajů a příslušnými právními předpisy). U každého kodexu je určen subjekt, který jej spravuje (zpravidla předkladatel kodexu), jehož úkolem je zajistit v dalším časovém období aktuálnost kodexu chování v souvislosti s rozvojem technologií, nově zaváděnými postupy správců či zpracovatelů nebo změnou právních předpisů.

Postup bude shodný v případě návrhu nového kodexu i návrhu úprav/změny stávajícího kodexu a lze ho rozdělit do čtyř základních částí:

- doporučeným krokem je oznámení zahájení prací na přípravě kodexu (základní informace o zpracovateli a předmětu kodexu), aby Úřad pro ochranu osobních údajů mohl učinit kroky nezbytné pro posouzení, vydání stanoviska a schválení návrhu

[2] článek 41 nařízení 2016/679

[3] V rámci zajištění jednotného uplatňování obecného nařízení se očekává v této věci stanovisko Sboru. Teprve až budou vytvořeny a schváleny akreditační požadavky, bude možné přijímat žádosti o akreditaci. Úřad o tom bude veřejnost včas informovat.

kodexu, případně i přípravu požadavků na akreditaci subjektů pro monitorování příslušného kodexu chování,[4]

- zajištění nezbytných konzultací týkajících se formy, obsahu a náležitostí kodexu na základě poptávky zpracovatele kodexu vůči Úřadu pro ochranu osobních údajů,
- předložení výsledného návrhu kodexu Úřadu pro ochranu osobních údajů k vydání stanoviska a schválení,
- registrace kodexu (obsahuje procesy spojené s jeho schvalováním a zveřejněním).[5]

Struktura kodexu

Kodex musí být zpracován tak, aby pokryl požadavky upravené obecným nařízením o ochraně osobních údajů pro (operace) zpracování osobních údajů konkrétního druhu. Text kodexu Úřad doporučuje rozčlenit na části odpovídající článkům obecného nařízení (upravujícím činnost správce nebo zpracovatele při zpracování osobních údajů) a v jejich rámci pak definovat postupy a požadavky na zpracování osobních údajů, a to jak pozitivní (co správce nebo zpracovatel dělat musí), tak negativní (co správce nebo zpracovatel dělat nesmí).

Příklad struktury kodexu chování

1. Název kodexu chování.
2. Verze dokumentu a platnost dokumentu (od data).
3. Určení správců, na které se kodex chování vztahuje (případně zpracovatelů).
4. Určení územní působnosti kodexu.
5. Popis (operací) zpracování, na které se kodex vztahuje:
    - popis (operací) zpracování
    - definice a popis účelů zpracování, které správce zpracováním osobních údajů sleduje,
    - rozsah údajů, které budou zpracovány (minimalizace rozsahu), a případně i právní předpisy upravující zpracování osobních údajů,
    - doba uchování údajů,
    - předávání osobních údajů (subjekty údajů, zpracovatelé, správci, předávání do zahraničí).
6. Postupy pro zajištění aktualizace a přesnosti údajů.
7. Postupy pro zajištění zákonnosti zpracování.
8. Postupy pro zajištění souhlasu subjektů údajů (včetně případného souhlasu dětí a jejich zákonných zástupců).
9. Postupy pro zajištění informovanosti subjektu údajů a veřejnosti.
10. Postupy pro zajištění a výkon práv subjektů údajů:
    - na přístup k osobním údajům,
    - na opravu osobních údajů a doplnění neúplných osobních údajů,
    - na výmaz osobních údajů (právo být zapomenut),
    - na omezení zpracování osobních údajů,

[4] článek 43 odst. 3 a článek 57 odst. 1 písm. p) nařízení 2016/679

[5] Podrobněji viz kap. Schválení a zveřejnění kodexu

- na přenositelnost údajů,
- na vznesení námitky proti zpracování osobních údajů,
- nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování,
- na podání stížnosti u Úřadu pro ochranu osobních údajů,
- na soudní ochranu vůči správci či zpracovateli (včetně postupů při mimosoudním vyrovnání a dalších jednání mezi správci a subjekty údajů).

11. Postupy pro zajištění bezpečnosti osobních údajů:
    - posouzení bezpečnosti,
    - soubor technických a organizačních opatření (řízení fyzického přístupu, řízení logického přístupu, zajištění čitelnosti osobních údajů oprávněnými osobami (včetně šifrování), logování a monitorování, použití identifikace a autentizace, použití hesel, zabezpečení komunikačního prostředí, zajištění funkčnosti, zálohování, archivace, kontinuita činnosti/obnova po mimořádné situaci, likvidace dat a datových nosičů, personální opatření atd.),
    - způsob a periodicita ověření účinnosti přijatých technických a organizačních opatření,
    - dokumentace k zajištění bezpečnosti (bezpečnostní politika, analýza rizik a posouzení vlivu na ochranu osobních údajů, dokumentace technických a organizačních opatření, dokumentace vývoje produktu, inventarizace hardware, software, služeb, dat a médií apod.).
12. Postupy při zpracování osobních údajů správcem nebo zpracovatelem se sídlem mimo EU, pokud k němu bude docházet.
13. Postupy při zajištění operací zpracování prostřednictvím zpracovatele, pokud se bude na zpracování podílet.
14. Postupy při zpracování záznamů o činnostech zpracování (případně, vzorové vyplnění), pokud je třeba je zpracovávat.
15. Postupy pro organizaci a řešení porušení zabezpečení osobních údajů.
16. Posouzení vlivu na ochranu osobních údajů (zásady, případně vzorové zpracování), pokud je třeba zpracovávat.
17. Postupy zřízení a činnosti pověřence pro ochranu osobních údajů, pokud bude jmenován.
18. Postupy při předávání osobních údajů do třetích zemí nebo mezinárodním organizacím, pokud k němu bude docházet.
19. Postupy pro monitorování kodexu chování u správce nebo zpracovatele.
20. Vzor doložky obsahující závazek subjektu k dodržování kodexu a zajištění monitorování kodexu, případně i na další spolupráci s akreditovaným subjektem.

Schvalování a zveřejnění kodexu

Kodex probíhá schvalovací procedurou v závislosti na tom, jaké území zasahuje:

Pokud se kodex vztahuje pouze na subjekty v rámci jednoho členského státu (v tomto případě České republiky), předloží zpracovatel jeho návrh dozorovému úřadu (v tomto případě Úřadu pro ochranu osobních údajů). Úřad vydá stanovisko, zda je nebo není kodex v souladu s obecným nařízením o ochraně osobních údajů. Pokud kodex je v souladu s obecným

nařízením o ochraně osobních údajů, Úřad pro ochranu osobních údajů kodex schválí, zaregistruje a zajistí jeho zveřejnění.[6]

Pokud se kodex vztahuje/může vztahovat na subjekty v rámci více členských států Evropské unie, předloží zpracovatel jeho návrh Úřadu pro ochranu osobních údajů. Ten kodex postoupí Sboru, který vydá stanovisko, zda je nebo není kodex v souladu s obecným nařízením o ochraně osobních údajů. Pokud kodex je v souladu s obecným nařízením o ochraně osobních údajů, předloží Sbor své stanovisko Komisi, která může rozhodnout o jeho všeobecné platnosti a zajistí jeho zveřejnění.[7]

Akreditace a monitorování kodexu

Jelikož se v případě kodexů jedná o samoregulační nástroj, nařízení počítá s tím, že dodržování kodexu chování bude monitorováno buď samotným dozorovým úřadem, nebo subjektem akreditovaným dozorovým úřadem.

Monitorování dodržování kodexu bude provádět subjekt akreditovaný[8] Úřadem pro ochranu osobních údajů a zvolený správcem nebo zpracovatelem. Osvědčení o akreditaci vydává Úřad všem subjektům, které splní požadavky pro akreditaci subjektů pro monitorování kodexů. Platnost akreditace je 5 let. Úřad pro ochranu osobních údajů může za určitých podmínek akreditaci také zrušit.[9]

Z důvodů již výše uvedených není prozatím možné žádat Úřad o akreditaci. Nicméně z důvodů úplnosti informací a také vzhledem k zájmu veřejnosti o tuto problematiku jsou níže uvedeny základní postupy a požadavky pro akreditaci, které mohou být ovšem korigovány očekávaným stanoviskem Sboru.

1. Požadavky pro akreditaci subjektů pro monitorování kodexů

Akreditace se provádí na základě požadavků připravených Úřadem pro ochranu osobních údajů a schválených Sborem[10] v rámci zajištění jednotného uplatňování obecného nařízení o ochraně osobních údajů v zemích Evropské unie.

Je třeba předeslat, že příprava požadavků pro akreditaci subjektů pro monitorování kodexů chování není krátkodobý proces. Obecně lze předpokládat, že kromě obecných požadavků (nestrannost, kvalita, bezdlužnost, čistý trestní rejstřík), požadavků na odbornost v oblasti bezpečnosti a ochrany osobních údajů, budou formulovány i požadavky na odbornost týkající se činnosti dané skupiny správců či zpracovatelů (znalost právních předpisů např. v oblasti zdravotnictví apod.). Pokud předkladatel kodexu nebude Úřad předběžně informovat o práci na přípravě kodexu, dá se očekávat zahájení prací na požadavcích pro akreditaci až po

[6] článek 40, odst. 5 a 6 nařízení 2016/679
[7] článek 41 odst. 7, 8, 9 a 10 nařízení 2016/679
[8] článek 41 odst. 1 nařízení 2016/679
[9] článek 41 odst. 5 nařízení 2016/679
[10] článek 64 odst. 1 písm. c nařízení 2016/679

předání kodexu. Tím nepochybně dojde k prodloužení termínu, kdy bude kodex chování připraven k uplatnění v praxi.

Seznam akreditovaných subjektů s uvedením seznamu kodexů, pro které jsou oprávněny provádět monitorování, uveřejní Úřad pro ochranu osobních údajů na svých webových stránkách. Pokud subjekt přestane dodržovat požadavky pro akreditaci nebo provádí monitorování dodržování kodexu v rozporu se schválenými postupy nebo obecným nařízením o ochraně osobních údajů, Úřad pro ochranu osobních údajů jeho akreditaci zruší. Subjektu může rovněž vypršet platnost akreditace nebo může oznámit Úřadu pro ochranu osobních údajů ukončení nebo přerušení činnosti.

2. Přijetí závazku a monitorování dodržování kodexu

K dodržování schváleného kodexu, který bude uveřejněn na webových stránkách Úřadu pro ochranu osobních údajů, se může přihlásit jakýkoliv subjekt, který patří do skupiny subjektů s obdobným charakterem činnosti, pro které je kodex určen. Závazek k dodržování kodexu a závazek k zajištění monitorování kodexu musí být součástí textu kodexu, který statutární zástupce subjektu podepíše a opatří značkou/razítkem subjektu. Originál kodexu opatřený podpisem a razítkem/značkou musí být k dispozici u subjektu, který se k jeho dodržování přihlásil.

Po podpisu kodexu správce nebo zpracovatel zajistí monitorování dodržování kodexu nezávislým a nestranným subjektem[11] akreditovaným Úřadem pro ochranu osobních údajů. Výběr provede správce nebo zpracovatel vhodným způsobem ze subjektů uvedených na seznamu uveřejněném na webových stránkách Úřadu. Monitorování je prováděno za úplatu, ceník zveřejní akreditovaný subjekt.

V případě orgánů veřejné moci a veřejných subjektů se monitorování dodržování kodexu chování nezávislým a nestranným subjektem akreditovaným Úřadem pro ochranu osobních údajů neprovádí.[12] Místo toho může provádět monitorování pověřenec pro ochranu osobních údajů nebo vnitřní kontrolní orgán orgánu veřejné moci nebo veřejného subjektu.

Monitorování dodržování kodexu by se mělo provádět minimálně s roční periodicitou (bude ještě upřesněno). O výsledku monitorování se zpracovává monitorovací/auditní zpráva. Poslední dvě monitorovací zprávy uchovává správce nebo zpracovatel pro případnou kontrolu Úřadem pro ochranu osobních údajů.

Stížnost na činnost akreditovaného subjektu pro monitorování kodexu musí být adresována Úřadu pro ochranu osobních údajů.

3. Povinnosti subjektů akreditovaných pro monitorování kodexů

Z povinností spojených s akreditací a prováděním monitorování kodexů chování je nutno zdůraznit, že subjekty pro monitorování kodexů musí být připraveny řešit podněty týkající se:

- jejich postupu a výrokům v rámci monitorování kodexů chování,

[11] článek 41 odst. 1 nařízení 2016/679
[12] článek 41 odst. 6 nařízení 2016/679

- nedodržování kodexů chování jednotlivými subjekty, které se k jejich monitorování přihlásily.

Subjekty pro monitorování kodexů sdělují Úřadu pro ochranu osobních údajů přehled monitorovaných kodexů s uvedením opatření uplatněných vůči správci nebo zpracovateli a důvody jejich přijetí.[13]

[13] článek 41 odst. 4 nařízení 2016/679