KAPITOLA IV
SPRÁVCE A ZPRACOVATEL

Praktické shrnutí čl. 24 a 25

Články 24 a 25 Nařízení upravují odpovědnost správce a záměrnou a standardní ochranu osobních údajů. Odpovědnost správce dle čl. 24 Nařízení spočívá především v tom, že je povinen dodržovat všechny povinnosti plynoucí z Nařízení, a k tomu musí zavést vhodná technická a organizační opatření, přičemž povaha takových opatření je podmíněna různou mírou závažnosti rizika pro práva a svobody subjektů, které je nutné analyzovat. Soulad s Nařízením musí být správce schopen i prokázat, a to zejména příslušnou dokumentací.

Čl. 25 Nařízení pak upravuje záměrnou a standardní ochranu osobních údajů, přičemž každý z těchto institutů slouží jiným způsobem k ochraně práv a svobod subjektů údajů. Záměrná ochrana osobních údajů spočívá v přijímání vhodných technických a organizačních opatření při určení prostředků pro zpracování i v době zpracování samotného, a to na základě posouzení závažnosti rizik pro práva a svobody subjektů údajů. Tím by měla být individuálně zajištěna optimální ochrana osobních údajů s přihlédnutím ke specifickým aspektům každého procesu. Standardní ochrana osobních údajů spočívá v povinnosti správce přijmout vhodná organizační a bezpečnostní opatření k zajištění toho, aby byly pro daný účel standardně zpracovány jen osobní údaje nezbytně nutné. To také koresponduje se zásadami minimalizace údajů a omezení uložení, avšak správce je povinen přijmout konkrétní opatření k provedení těchto zásad.

Jednou z hlavních povinností, kterou úprava v čl. 24 a 25 Nařízení ukládá správci, je aktivní dokládání souladu, resp. možnost prokázat soulad zpracování s Nařízením dle čl. 24 odst. 1 Nařízení. Nejvhodnější formou prokazování je pak dokumentace vedená správcem prokazující soulad zpracování osobních údajů s povinnostmi plynoucími z Nařízení. Nutnost proaktivního přístupu správce se pak promítá například do nutnosti provádět zabezpečení zpracování, posouzení vlivu nebo předchozí konzultace.

Pro zajištění souladu lze správcům doporučit především revizi a případné zavedení interních směrnic na ochranu osobních údajů a všech vnitřních dokumentů týkajících se zpracování osobních údajů a úpravu vedení dokumentace tak, aby z ní vyplýval soulad zpracování s Nařízením.

S ohledem na záměrnou ochranu osobních údajů lze správcům dále doporučit zejména analýzu rizik u zpracování a následné zavedení opatření, kterými mohou být například pseudonymizace, omezení přístupu nebo fyzické a síťové zabezpečení údajů. Také lze doporučit stanovení vnitřních pravidel získávání a zpracování osobních údajů tak, aby byla zajištěna standardní úroveň ochrany.

Oddíl 1 Obecné povinnosti

Čl. 24 Odpovědnost správce

1. **S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.**
2. **Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uvedená v odstavci 1 uplatňování vhodných koncepcí v oblasti ochrany údajů správcem.**
3. **Jedním z prvků, jimiž lze doložit, že správce plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42.**

Body odůvodnění: 74, 75, 76, 77, 83

Sankce: čl. 83 odst. 4 písm. a) Nařízení

I. Provádění principu odpovědnosti

Jak je vysvětleno již v komentáři k čl. 5 v části X, odpovědnost jakožto (1) povinnost zajistit soulad s Nařízením a (2) povinnost být schopen tento soulad aktivně prokázat se stala v nové úpravě klíčovým principem, jehož účelem je zajišťovat skutečně efektivní způsob provádění ostatních základních zásad Nařízení. K tomuto účelu Nařízení zakotvuje v části IV několik konkrétních institutů. Jsou to zejména technická a organizační opatření pro soulad s Nařízením dle čl. 24 Nařízení, zásada záměrné a standardní ochrany osobních údajů dle čl. 25 Nařízení, vedení záznamů o zpracování dle čl. 30 Nařízení, posouzení vlivu na ochranu osobních údajů dle čl. 35 Nařízení, předchozí konzultace podle čl. 36 Nařízení a pověřenec pro ochranu osobních údajů dle čl. 37–39 Nařízení.

Klíčovou složkou principu odpovědnosti je v souladu s čl. 24 odst. 1 Nařízení přijímání technických a organizačních opatření pro **zajištění souladu** s Nařízením a **schopnosti soulad prokázat** na základě komplexního posouzení, ve kterém správce přihlédne k povaze, rozsahu, kontextu a účelům zpracování a k různě závažným a pravděpodobným rizikům pro práva a svobody, která zpracování představuje.

Orientace právní oblasti ochrany osobních údajů na riziko je celosvětovým trendem, který se projevuje již řadu let. V roce 2013 došlo k velké aktualizaci nezávazné směrnice OECD[1], ve které bylo zohlednění rizik označeno za jeden z hlavních principů, na kterém by měla být ochrana osobních údajů postavena. V současné úpravě se posuzování rizika také objevuje, avšak pouze v omezené míře, při určování vhodných prostředků zabezpečení osobních údajů.[2] Zásada odpovědnosti se potom celkově odráží zejména v povinnosti oznamovat zpracování osobních údajů dozorovému úřadu.

V Nařízení je koncept odpovědnosti značně rozpracován a je v tomto směru posílena role správce a zpracovatele. Praxe uplatňování směrnice ukázala, že ačkoli jsou zpracování oznamována dozorovým úřadům, jejich schopnost

[1] Původní směrnice OECD z roku 1980 de facto určila podobu nejvýznamnějších institutů ochrany osobních údajů tak, jak jsou používány dodnes. V roce 2013 došlo k významné aktualizaci, která reaguje na změny, ke kterým došlo v této oblasti za předchozích 30 let. Aktualizace přinesla do směrnice dva základní prvky. Prvním z nich je právě zaměření na řízení rizika, druhým pak potřeba spolupráce a interoperability v globalizovaném světě. OECD. *The OECD Privacy Framework* [online]. 2013 [cit. 2017-03-31]. Dostupné z: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[2] § 13 odst. 3 zák. o ochraně os. údajů.

efektivně kontrolovat veškerá oznámená zpracování je omezená. Z toho důvodu Nařízení ukládá správci (a v omezeném rozsahu i zpracovateli), aby posoudil rizika pro práva a svobody fyzických osob, která jsou se zpracováním spojena, a podle významu těchto rizik uplatnil některá opatření k zajištění souladu s Nařízením.

II. Rizika pro práva a svobody fyzických osob

Posouzení rizika zpracování osobních údajů je určujícím prvkem při provádění povinností dle Nařízení. Nařízení v tomto směru požaduje, aby způsob zajišťování souladu s jeho pravidly vždy odpovídal riziku, které prováděné zpracování představuje pro práva a svobody fyzických osob. Tímto pravidlem se musí správce řídit při přijímání organizačních a technických opatření s cílem zajistit provádění všech zásad pro zpracování, jako je minimalizace údajů, přesnost, omezení uložení či důvěrnost a integrita, ale také např. při zavádění procesů pro výkon práv subjektů údajů nebo při výběru vhodných zpracovatelů.

Riziko pro práva a svobody fyzických osob se v Nařízení objevuje zároveň také jako kritérium, na němž závisí uplatnění nebo míra uplatnění řady institutů. S posuzováním rizika se úzce pojí provádění principu odpovědnosti, kvůli kterému musí být správce schopen doložit soulad s Nařízením. Správce by tak měl všechna provedená posouzení rizik a následné zvolení vhodných opatření k jejich zmírnění pečlivě odůvodnit a přiměřeně zdokumentovat pro potřeby prokazování souladu.

Posouzení rizik pro práva a svobody fyzických osob je nutné provádět zejména při:

a) zavádění opatření k zajištění schopnosti doložit soulad s Nařízením dle čl. 24 Nařízení,
b) zpracování na základě oprávněného zájmu správce v rámci balančního testu dle čl. 6 odst. 1 písm. f) Nařízení,
c) posouzení slučitelnosti účelů v rámci vyhodnocování důsledků dalšího zpracování dle čl. 6 odst. 4 písm. d) Nařízení,
d) zavádění ochranných opatření v souvislosti s automatizovaným individuálním rozhodováním dle čl. 22 odst. 3 Nařízení,
e) provádění principů záměrné ochrany osobních údajů dle čl. 25 Nařízení,
f) posuzování aplikace výjimky z nutnosti vedení záznamů o zpracování dle čl. 30 Nařízení,
g) přijímání technických a organizačních opatření k zabezpečení osobních údajů dle čl. 32 Nařízení,

h) posuzování nutnosti ohlásit porušení zabezpečení osobních údajů dle čl. 33 a 34 Nařízení,
i) posuzování vlivu na ochranu osobních údajů dle čl. 35 Nařízení,
j) posuzování nutnosti předchozí konzultace dle čl. 36 Nařízení,
k) posuzování nutné kvalifikace pověřence pro ochranu osobních údajů dle čl. 37 odst. 5 Nařízení nebo
l) určování priorit práce pověřence pro ochranu osobních údajů dle čl. 39 odst. 2 Nařízení.

Nařízení obecně rozpoznává tři druhy rizika pro práva a svobody, které mají odraz v uplatnění či míře uplatnění jednotlivých výše uvedených povinností:

a) **Riziko.** Riziko je obecným měřítkem zavádění technických a organizačních opatření k plnění povinností v Nařízení. Posouzení rizika je komplexní analýza zaměřená na zjištění možné újmy pro subjekty údajů a pravděpodobnosti, s jakou újma může vzniknout. Na základě analýzy musí správce následně přijmout taková opatření, aby riziko co nejvíce zmírnil. Kromě institutů, u nichž je výslovně zmíněno, je nutné je uplatňovat všude, kde je na správci, aby zavedl nějaký systém pro soulad s Nařízením. Příkladem může být např. zásada přesnosti. Je na správci, aby posoudil, jak často je s ohledem na riziko nutné přesnost osobních údajů ověřovat. Stejně tak musí správce s ohledem na riziko vyvinout vhodné způsoby pro uplatňování práv subjektů údajů.
b) **Vysoké riziko.** Pokud na základě posouzení rizika správce zjistí, že při zpracování hrozí vysoké riziko, aktivuje se pro něj povinnost provést posouzení vlivu na ochranu osobních údajů dle čl. 35 Nařízení, povinnost provést předchozí konzultace s dozorovým úřadem dle čl. 36 Nařízení a v případě porušení zabezpečení osobních údajů povinnost notifikovat subjekty údajů dle čl. 34 Nařízení. Za vysoce rizikové zpracování bude považováno např. zpracování, které v souladu s dosaženou úrovní technických znalostí využívá nových technologií, jakož i jiných operací zpracování, které představují vysoké riziko pro práva a svobody subjektů údajů, zejména v případech, kdy je pro subjekty údajů s ohledem na tyto operace obtížnější uplatnit svá práva.[3]
c) **Nízké riziko.** Nízké riziko aktivuje některé výjimky z povinností dle Nařízení. Nízké riziko tak může správce zprostit povinnosti ohlašovat

[3] Bod 91 odůvodnění Nařízení.

porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 Nařízení a správce ze třetí země mimo EU může nízké riziko zprostit povinnosti jmenovat zástupce v EU dle čl. 27 Nařízení.

Existuje více doporučovaných metodik pro posuzování rizik v oblasti osobních údajů, např. metodiky vydané francouzským dozorovým úřadem CNIL[4] nebo britským ICO[5]. Tyto metodiky svou šíří nepokrývají komplexní přístup, který k posuzování rizik zaujímá Nařízení, základní principy pro určování rizika zpracování však zůstávají zachovány. Při určování rizika zpracování lze proto vycházet z následujícího postupu:

a) identifikace hrozeb spojených se zpracováním,
b) identifikace potenciální újmy dotčených osob spojené se zpracováním jejich osobních údajů,
c) zhodnocení pravděpodobnosti, že újma vznikne, posouzením slabých míst systémů a procesů zpracování oproti povaze hrozby,
d) zhodnocení závažnosti potenciální újmy, pokud by vznikla.

III. Identifikace hrozeb spojených se zpracováním

V rámci celého životního cyklu osobních údajů od jejich shromáždění do jejich likvidace mohou vznikat různé hrozby pro práva a svobody fyzických osob. Tyto hrozby je nutné při každém zpracování důsledně identifikovat, jelikož na jejich základě je poté prováděno celé posouzení rizik. Za takové hrozby přitom není považováno pouze porušení zabezpečení údajů, ale také různé hrozby, které může vyvolávat sám správce, například zpracováním údajů v rozporu se základními zásadami Nařízení. Mezi tyto hrozby může patřit např.:

a) zpracování osobních údajů v rozporu se zásadou zákonnosti,
b) nevhodné zpracování osobních údajů, které přesahuje rozumné očekávání subjektu údajů či které jde nad rámec obvyklého očekávání ve společnosti,
c) nezákonné překročení stanoveného účelu zpracování,

---

[4] CNIL. *Methodology for Privacy Risk Management: How to implement the Data Protection Act* [online]. [cit. 2017-03-31]. Dostupné z: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf.

[5] ICO. *Conducting privacy impact assessments, code of practice* [online]. [cit. 2017-03-31]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

d) rozpor se zásadou minimalizace údajů, tzn. excesivní shromažďování či jiné zpracování osobních údajů,
e) zpracování či uchovávání osobních údajů, které jsou nepřesné či neaktuální,
f) uchovávání osobních údajů po dobu delší, než je nutná,
g) narušení integrity či důvěrnosti osobních údajů nebo
h) znemožnění či ztížení možnosti uplatnit práva subjektů údajů.

Správce by přitom neměl posuzovat pouze újmu, kterou může způsobit zpracováním on sám, ale také újmu, která může subjektům údajů vzniknout následným jednáním třetí strany, např. po předání či zveřejnění osobních údajů.

IV. Identifikace potenciální újmy

Jakmile jsou identifikované hrozby, které jsou s daným zpracováním osobních údajů spojeny, je potřeba identifikovat potenciální újmu fyzickým osobám, která může v důsledku hrozeb vzniknout. Nařízení explicitně nestanoví úplný výčet újem, které je třeba brát v úvahu. Vodítko k identifikaci potenciální újmy však poskytuje bod 75 odůvodnění Nařízení, který říká, že rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy:

a) by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění nebo
b) by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje.

V. Zhodnocení pravděpodobnosti vzniku újmy

Jakmile je možná újma pro práva a svobody fyzických osob identifikována, je nutné posoudit její pravděpodobnost. Pravděpodobnost vzniku újmy je třeba určit posouzením pravděpodobnosti, že se realizuje hrozba a v jejím důsledku vznikne subjektům údajů předvídaná újma.

Míra pravděpodobnosti vzniku újmy bude záviset na faktorech, jakými jsou např.:

a) počet osob zapojených do zpracování,
b) zapojení třetích stran do zpracování,

c) rozdílné právní požadavky dopadající na zpracování osobních údajů (např. při předání osobních údajů do zahraničí),
d) slabá místa v procesech a systémech zpracování a nedostatky ve správě osobních údajů obecně nebo
e) historie předchozích incidentů, při nichž došlo ke vzniku újmy.

Příklad:

Nestátní registr dlužníků uchovává údaje o výši dluhů jednotlivých subjektů údajů, o kterých je informují různé subjekty, jako jsou banky, pojišťovny či mobilní operátoři. S ohledem na počet osob, jejichž údaje mohou být v takovém registru shromážděny, počet subjektů, od kterých jsou údaje získávány, a objem předávaných dat je pravděpodobnost nepřesnosti dat vysoká. Proto je vysoce pravděpodobné, že v tomto registru v důsledku nepřesnosti dat dojde např. k nesprávnému rozhodnutí, které může mít závažný dopad na subjekt údajů.

VI. Zhodnocení závažnosti potenciální újmy

Vedle posouzení pravděpodobnosti újmy je dalším důležitým krokem zhodnocení její závažnosti. Faktory, které určují závažnost újmy, jsou např.:

a) citlivost osobních údajů (přičemž se nelze omezit pouze na zvláštní kategorie osobních údajů dle čl. 9 Nařízení, ale je nutné zvažovat skutečnou citlivost údajů – např. platební údaje do této kategorie nespadají, ale velmi citlivé bezpochyby jsou),
b) objem zpracovaných osobních údajů,
c) zranitelnost dotčených fyzických osob,
d) možný dopad zpracování na významné události v životě fyzických osob nebo
e) možný dopad zpracování na finanční a ekonomickou situaci fyzických osob.

Zároveň je nutné posoudit benefity, které může určité zpracování – byť rizikové – pro subjekt údajů znamenat. V některých případech může být výhoda natolik velká, že ospravedlní zbytkové riziko, které není možné dostatečně zmírnit.