Metodika obecného posouzení vlivu na ochranu osobních údajů

Verze 1.0 ze dne 11. listopadu 2020

Obsah:

Metodika obecného posouzení vlivu na ochranu osobních údajů

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 „obecné nařízení o ochraně osobních údajů“ nebo jen „nařízení“) předpokládá v některých případech (článek 35) provedení posouzení vlivu na ochranu osobních údajů (dále jen „posouzení vlivu“). Nejde o povinnost zcela novou, i pro zpracování osobních údajů v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, platila povinnost posoudit rizika[1], přijmout[2] a dokumentovat[3] přijatá technická a organizační opatření.

Vzhledem k tomu, že existuje několik dokumentů upravujících buď přímo posuzování dopadů do soukromí[4], nebo postupy řízení rizik pro některé správce v rámci České republiky, kteří mohou zpracovávat osobní údaje s vysokými riziky pro práva a svobody subjektů údajů[5], je „Metodika posouzení vlivu na ochranu osobních údajů (dále též Metodika)“ připravena se záměrem Úřadu na:

- zajištění souladu s obecným nařízením o ochraně osobních údajů,
- snížení (administrativního) zatížení správců (využitím některých postupů a řešení, které jsou povinni používat ke splnění jiných povinností),
- respektování dalších odborných podkladů/dokumentů, které jsou k uvedené nebo obdobné problematice k dispozici.

Je třeba upozornit na to, že se jako součást návrhů právních předpisů podle článku 4 odst. 1 písm. g), článku 9 odst. 2 písm. h), článku 14 odst. 1 písm. g) a článku 16 odst. 4 legislativních pravidel vlády hodnotí dopady navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů. I v těchto případech se Metodika použije jako výchozí dokument. Je to proto, že § 10 zákona č. 110/2019 Sb., o zpracování osobních údajů, uvádí, že správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést. Nedílnou součástí návrhů právních předpisů musí být (jak bylo výše zmíněno) zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů, které by mělo obsahovat rovněž stanovení technických a organizačních opatření na ochranu osobních údajů, která umožní budoucímu správci a dalším subjektům implementaci a bezpečné zpracování osobních údajů. Navrhovaná technická a organizační opatření mohou být obecnější povahy

[1] § 13 odst. 3 zákona č. 101/2000 Sb.
[2] § 13 odst. 1 zákona č. 101/2000 Sb.
[3] § 13 odst. 2 zákona č. 101/2000 Sb.
[4] např. ČSN ISO/IEC 29134
[5] např. vyhláška č. 82/2018 Sb.

(pokud právní předpis upravuje zpracování osobních údajů prováděné více subjekty, například obcemi) a konkrétnější povahy (pokud právní předpis upravuje zpracování osobních údajů prováděné jedním správcem). Vzhledem k poněkud odlišným (rozšířeným) požadavkům pro předklad návrhů právních předpisů Úřad pro tento účel vypracoval „Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů“[6], který rozšiřuje Metodiku o některé specifické požadavky.

Posouzení vlivu by se mělo opakovaně přehodnocovat. Takže, i když se ke dni použitelnosti nařízení posouzení vlivu od správce nevyžaduje, bude správce ve vhodnou dobu (změna parametrů zpracování, nové hrozby, změna technologií apod.) nucen toto posouzení vlivu provést v rámci svých povinností obecné odpovědnosti.

Metodika je v souladu s čl. 35 nařízení určena primárně pro potřeby správců, ale mohou ji využít i zpracovatelé osobních údajů (pokud např. v rámci dodávky předloží typovou DPIA pro jimi dodávané produkty), dále zpracovatelé legislativních návrhů i další odborníci na ochranu osobních údajů.

Metodika má těmto subjektům přinést návod, jak provádět posouzení vlivu. Pokud by i přesto byl tento dokument náročný na aplikaci na jimi prováděná zpracování osobních údajů, doporučuje Úřad obrátit se o pomoc na specialistu na řešení uvedené problematiky.

Metodika představuje jeden z možných (a doporučených) postupů, jak zajistit soulad s obecným nařízením o ochraně osobních údajů. Správce může zvolit i odlišný postup, obsahově však musí splňovat alespoň požadavky dle čl. 35 odst. 7 nařízení.

Terminologie

Vzhledem k poněkud odlišné terminologii v oblasti kybernetické bezpečnosti (používaná v rámci právních předpisů) a ochrany osobních údajů (používaná v rámci právních předpisů nebo normách) je důležité definovat některé používané pojmy a vysvětlit vztah pojmů používaných v obou oblastech.

Zpracovatel – fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
(Poznámka: zpracovatel provádí jednu nebo více operací zpracování (například uchování, likvidace, ale i celé zpracování) osobních údajů namísto správce, a to z pověření správce, tj. stává se dodavatelem správce, ale ne všichni dodavatelé správce jsou zároveň zpracovatelé).

Sekundární/podpůrné aktivum – technické aktivum (HW, SW, komunikační prostředky, nosiče informací), objekty, zaměstnanci a dodavatelé (jejichž zvláštní skupinou jsou zpracovatelé osobních údajů), externí služby podílející se na provozu, rozvoji, správě nebo bezpečnosti (operací) zpracování osobních údajů.

[6] https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu-pravnich-predpisu-dpia/ds-5344/archiv=0&p1=1257.

Primární aktivum – informace (v tomto případě zejména osobní údaje nebo další údaje spojené se zpracováním osobních údajů) nebo služby (zajišťované procesy nebo činnosti, tedy i operace zpracování) v rámci zpracování osobních údajů.

K provádění posouzení vlivu v otázkách a odpovědích

Správci budou při přípravě zpracování osobních údajů řešit problémy související s tím, zda vůbec, kdo, kdy a v jakém rozsahu má posouzení vlivu provádět.

1) Proč posouzení vlivu provádět?

Pokud při zpracování osobních údajů dojde ke zničení, neoprávněné změně či znepřístupnění zpracovávaných osobních údajů, má to pro subjekty údajů (ale i správce) různé negativní důsledky (některé z nich i velmi závažné). Aby se jim zabránilo nebo se alespoň omezily, provádí se zabezpečení zpracování osobních údajů, a to prostřednictvím různých opatření (zejména technických a organizačních). Správcem přijatá opatření jsou volena s přihlédnutím k parametrům (povaha, rozsah, kontext a účely) zpracování osobních údajů, rizikům pro práva a svobody fyzických osob[7], stavu techniky a nákladům na jejich provedení. Výběr opatření by měl být prováděn tak, aby výsledkem bylo zajištění souladu zpracování osobních údajů s požadavky obecného nařízení o ochraně osobních údajů, zároveň však přijatá opatření nejsou nedostatečně účinná nebo nejsou nepřiměřeně nákladná.

2) Kdo posouzení vlivu provádí?

Posouzení vlivu provádí správci[8]. V některých případech (viz níže) může[9] posouzení vlivu provést i někdo jiný (např. dodavatel IT řešení nebo jedno posouzení pro více správců provede například dodavatel programového vybavení apod.). Nesnižuje to však vlastní odpovědnost správce za zpracování osobních údajů a řízení rizik.
(Poznámka: zpracované posouzení vlivu může být součástí dodávky uceleného programového vybavení. Pokud však jde jen o dílčí produkt, může správce čerpat (pro provedení posouzení svého) informace z posouzení vlivu vypracovaného poskytovatelem produktu, ale nemůže ho převzít jako hotovou věc, protože nepokrývá celé zpracování osobních údajů).

Všechny tyto subjekty neprovádí povinně posouzení vlivu u všech zpracování osobních údajů. Obecné nařízení o ochraně osobních údajů ukládá povinnost provádět posouzení vlivu pouze u takových zpracování, která mají za následek **vysoká rizika pro práva a svobody fyzických osob**.

[7] článek 35, odstavec 1
[8] článek 35, odstavec 1
[9] článek 35, odstavec 10, recitál bod 92

Posouzení vlivu se zpravidla připravuje pro (operace) zpracování osobních údajů (jeho hranice definuje správce – například to může být archivace osobních údajů, evidence docházky, personalistika, ale i celý provozní/ekonomický systém správce).

Pro soubor podobných (operací) zpracování (s obdobnými riziky) prováděných různými správci, umožňuje obecné nařízení o ochraně osobních údajů provést pouze jediné posouzení vlivu. Jedná se o následující případy:

- Soubor podobných (operací) zpracování podporovaný společnou aplikací pro správce v určitém odvětví nebo jeho segmentu[10] (například některá zpracování osobních údajů prováděná lékárnami).
- Soubor podobných (operací) zpracování podporovaný společnou aplikací pro horizontální činnost prováděnou různými správci v různých odvětvích[10].
- Soubor podobných (operací) zpracování, pokud bylo pro skupinu správců posouzení vlivu provedeno a přijato jako součást právního předpisu nebo v rámci jednoho projektu[11].
- Soubor podobných (operací) zpracování, pokud správce uplatňuje a dodržuje Úřadem schválený kodex chování (*Poznámka: posouzení vlivu bylo součástí přípravy kodexu chování*)[12].

Při zpracování osobních údajů prováděné společnými správci[13] je možné provést jediné posouzení vlivu, je však třeba, aby byly:

- vyjádřeny potřeby jednotlivých společných správců při zpracování osobních údajů,
- vymezeny sdílené informace,
- vymezeny povinnosti jednotlivých správců při zpracování osobních údajů,
- všemi společnými správci určeny (a schváleny) hrozby a zranitelnosti zpracování osobních údajů,
- vymezeny odpovědnosti za implementaci jednotlivých opatření.

3) Kdy se posouzení vlivu provádí?

Posouzení vlivu se provádí před zahájením zpracování osobních údajů. V případě již existujících (před datem účinnosti obecného nařízení o ochraně osobních údajů) zpracování osobních údajů je nutno posouzení vlivu provést nejpozději při první změně rizika, které může vznikat např.:

- změnami parametrů zpracování,
- použitím nových technologií,
- změnami právních předpisů,
- expanzí správce (územní nebo organizační)

[10] recitál bod 92
[11] článek 35, odstavec 10, recitál bod 92
[12] článek 35, odstavec 8
[13] článek 26

- vznikem nových/neznámých hrozeb pro zpracování osobních údajů,
- jako součást řešení porušení zabezpečení osobních údajů.

Nicméně v případě již existujících zpracování osobních údajů lze doporučit, pokud půjde o zpracování osobních údajů velkého rozsahu nebo nasazení vysoce inovativního řešení, provést předběžné posouzení již v době formulace záměru, aby nedošlo ke zbytečně vynaloženým prostředkům v dalších fázích přípravy.
Monitorovaní a přezkoumávání rizik (respektive jejich změny) pro práva a svobody subjektů údajů probíhá soustavně. Zda je zpracování osobních údajů prováděno v souladu s posouzením vlivu na ochranu osobních údajů, by mělo být prověřováno i při změně rizika[14].
Monitorování uplatnění posouzení vlivu, včetně dodržování opatření a revize posouzení vlivu, může být prováděno v rámci plánovaných auditů nebo mimořádných auditů (po proběhlé mimořádné události, tj. porušení zabezpečení osobních údajů[15]). K tomu Pokyny WP248 na straně 16 uvádějí: V rámci osvědčených postupů by mělo být posouzení vlivu soustavně přezkoumáváno a mělo by se pravidelně přehodnocovat. Takže i když se ke dni použitelnosti nařízení posouzení vlivu nevyžaduje, správce bude ve vhodnou dobu nucen toto posouzení vlivu provést v rámci svých povinností obecné odpovědnosti.
Revize posouzení vlivu má zásadní význam pro udržení úrovně ochrany osobních údajů v postupně se měnícím prostředí.

4) Je třeba posouzení vlivu dokumentovat?

Správce je povinen nejen zavést vhodná technická a organizační opatření, ale i doložit, že zpracování osobních údajů je prováděno v souladu s obecným nařízením o ochraně osobních údajů[16]. Proto je třeba posouzení vlivu nejen zpracovat, ale i dokumentovat a uchovat (například pro účely dohledové činnosti).

5) Jak se posouzení vlivu provádí?

Minimální obsah posouzení vlivu upravuje[17] obecné nařízení o ochraně osobních údajů. Metodika upřesňuje možný způsob provádění (a obsah) posouzení vlivu, který je rozdělen na čtyři etapy:

1.etapa – shromáždění informací o zpracování osobních údajů, včetně správcem uplatněných mechanizmů pro doložení souladu s obecným nařízením o ochraně osobních údajů.

2.etapa – analýza (na základě informací dle předchozí odrážky), zda je nezbytné provést posouzení vlivu[18].

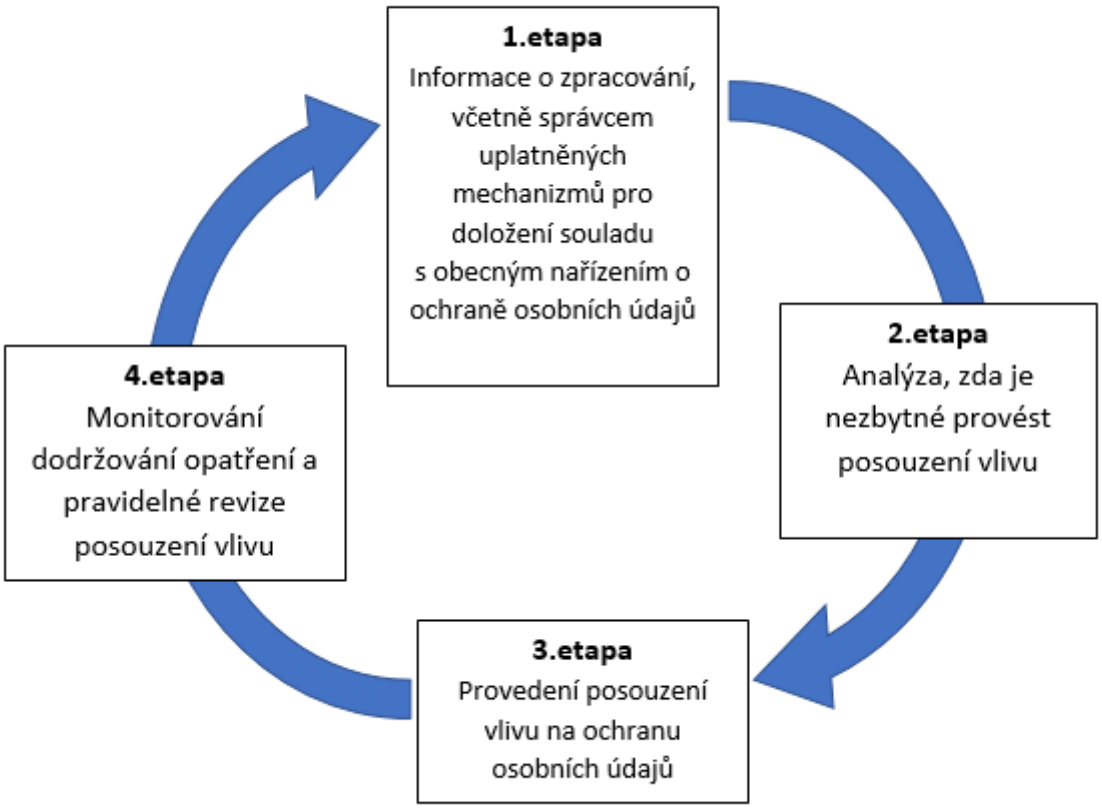
3.etapa – provedení posouzení vlivu.

[14] článek 35, odstavec 11
[15] článek 33, odstavec 3, písmeno d)
[16] článek 24, odstavec 1
[17] článek 35, odstavec 7
[18] materiál Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů

4.etapa – monitorování dodržování opatření a pravidelné revize posouzení vlivu.

Provedení posouzení vlivu

Jak bylo uvedeno výše, lze postup správce rozdělit do čtyř etap (viz obrázek 1). Každá obsahuje soubor kroků, které směřují k zajištění povinnosti provést posouzení vlivu. Podrobný rozpis postupu je uveden v Příloze 1.



Obr. 1 Schéma postupu správce

1. etapa
Informace o zpracování

Pro provedení analýzy, zda je či není správce povinen provést posouzení vlivu, je nezbytné mít k dispozici určité informace o zpracování osobních údajů. Postačují informace v rozsahu – popis vlastního zpracování, účel/y zpracování osobních údajů (včetně odůvodnění jeho legitimity dle čl. 6 odst. 1 písm. f) nařízení), subjekty údajů (druh a počet), zpracovávané osobní údaje (druh, rozsah a tok dat), doba uchování údajů, předávání osobních údajů jiným subjektům, zajištění práv a povinností subjektů údajů apod. V zásadě lze vyjít ze záznamů

o činnostech zpracování[19], které musí každý správce vést (pokud neprovádí nahodilá shromažďování osobních údajů, které dále nezpracovává).

2. etapa
Analýza, zda je nezbytné provést posouzení vlivu

Povinnost provést posouzení vlivu je uložena správcům, kteří provádějí zpracování osobních údajů mající za následek vysoká rizika pro práva a svobody fyzických osob (nicméně analýzu směřující k přijetí přiměřených opatření k zabezpečení zpracování osobních údajů by měl provést každý správce). Určení, zda se na správce tato povinnost vztahuje, lze provést ve dvou krocích, které je nutno zdokumentovat:

1. krok – nahlédnutí seznamu druhů operací zpracování, která nepodléhají posouzení vlivu, který Úřad připravil a je k dispozici **zde**. Seznam podléhá schválení Evropským sborem pro ochranu osobních údajů a může zaznamenat určité změny.

2. krok – pokud správce výjimku nemá (nenalezne zpracování osobních údajů na seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů), potom by měl provést vlastní hodnocení rizikovosti zpracování osobních údajů na základě parametrů jím prováděného zpracování osobních údajů a seznamu operací (seznam je zpracován jako parametrický), které mohou podléhat požadavku na posouzení vlivu. Tento seznam Úřad připravil a je k dispozici **zde**. Seznam podléhá schválení Evropským sborem pro ochranu osobních údajů a může zaznamenat určité změny.

3. etapa

Provedení posouzení vlivu

Vlastní posouzení vlivu lze rozdělit do osmi částí, v jejichž rámci správce provádí řadu činností.

1. část – systematický popis zamýšlených operací zpracování

- název a identifikace správce/sdílených správců,
- název a krátký popis (operací) zpracování osobních údajů,
- určení osob odpovědných za zpracování osobních údajů (údajů a operací zpracování),
- přehled funkčních požadavků na (operace) zpracování osobních údajů,
- seznam závazných právních předpisů a závazků správce,
- popis účelů (operací) zpracování osobních údajů (pokud je účelem povinnost uložená zákonem, musí být uvedeno, který zákon a který § povinnost ukládá s ohledem na nezbytnost a přiměřenost operací),
- seznam zpracovávaných údajů (v řadě případů totiž nepostačují pro provedení analýzy kategorie[20] osobních údajů),
- předpokládaná doba uchování osobních údajů,

[19] článek 30

[20] kategorií osobních údajů se rozumí například identifikační údaje nebo zvláštní kategorie osobních údajů nebo provozní údaje, vlastními osobními údaji se rozumí jméno, příjmení, údaj o členství v odborových organizacích, datum, navštívená webová stránka apod.

- kategorie subjektů údajů (například zaměstnanci, studenti, příjemci dávek, pacienti apod.),
- kategorie příjemců osobních údajů (subjekty mimo správce – zpracovatelé, předávání do zahraničí, předávání na základě právních předpisů) a způsob užití osobních údajů,
- zamýšlená opatření k doložení souladu, tj. informace o postupech správce ovlivňujících dodržení obecného nařízení o ochraně osobních údajů (dodržování kodexu chování, vydaná osvědčení (certifikace), uzavřené standardní smluvní doložky, schválené BCR (Binding Corporate Rules, tj. závazná podniková pravidla) apod.),
- popis zajištění práv subjektů údajů,
- diagram (workflow) popisující zpracování (tok) osobních údajů, včetně případných vazeb na jiná zpracování osobních údajů,
- určení agend a útvarů zajišťujících zpracování osobních údajů.

2. část – posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů, a to prostřednictvím testu proporcionality, který vyjadřuje:

- zda je zpracování osobních údajů s navrženými parametry nezbytné pro zajištění správcem definovaného/definovaných účelů,
- zda nelze využít jiný, efektivnější prostředek k zajištění definovaného účelu, než představuje navržené zpracování osobních údajů,
- zda uvedené zpracování osobních údajů zasahuje do soukromí osob pouze v nezbytně nutné míře.

3. část – posouzení rizik pro práva a svobody subjektů údajů

Příkladem posouzení rizik pro práva a svobody subjektů údajů je následující postup. Posouzení doporučujeme synchronizovat s obecnou analýzou rizik (viz například povinnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti), a to proto, že v rámci analýzy rizik vzniká kromě seznamu rizik pro dané zpracování údajů také seznam opatření, jak tato rizika eliminovat. To by, při oddělené analýze, mohlo vést k určitým nekonzistentnostem z hlediska přijatých opatření.

1. krok – identifikace a evidence primárních aktiv a sekundárních/podpůrných aktiv vztažených ke zpracování osobních údajů a identifikace a hodnocení vazeb mezi nimi.

2. krok – určení zranitelností

správce identifikuje zranitelnosti sekundárních/podpůrných aktiv, prostřednictvím jichž jsou realizovány hrozby (příklady viz Příloha 2).

(Poznámka: různá sekundární/podpůrná aktiva mohou mít stejnou zranitelnost).

3. krok – určení hrozeb

správce identifikuje relevantní hrozby, které se mohou využít zranitelností určených ve 2. kroku (příklady viz Příloha 3).

(Poznámka: Jedna hrozba může být realizována prostřednictvím více zranitelností a také jednu zranitelnost může využívat více hrozeb).

4. krok – prvotní určení míry rizika

V rámci posouzení rizik pro práva a svobody fyzických osob pro každou hrozbu uvést, jak se projeví na zpracovávaných osobních údajích a kvantifikovat míru rizika pro zpracovávané osobní údaje pomocí hodnocení dopadů, míry hrozeb a míry zranitelností. Míru rizika určuje správce postupem dle Přílohy 5. V zásadě může míra rizika u jednotlivých hrozeb pro osobní údaje nabývat hodnot mezi 1 (1x1x1) až 64 (4x4x4).

Pokud se jedná o zcela nové zpracování osobních údajů nebo kvalitativní (skokovou) změnu, uvažuje se míra rizika před redukcí, tzn. že žádná opatření nebyla přijata, nebo vzhledem ke skokové změně nejsou použitelná. V rámci tohoto přístupu lze předpokládat, že hodnocení míry zranitelnosti, míry hrozby a z toho následně vypočtená míra rizika se bude pohybovat na vyšší úrovni, např. vysoké nebo kritické riziko. Taková rizika vyžadují další zásahy (redukci míry rizika např. prostřednictvím technických a organizačních opatření).

5. krok – ošetření rizik (způsob řešení rizik a přijetí opatření k řešení rizik).
Z posouzení vlivu vyjde v některých případech riziko jako kritické, vysoké nebo střední. Možností redukce rizika pro zpracovávané osobní údaje je několik.

- Snížení rizika – přijetí opatření na straně správce, tak aby míra rizika byla snížena na přijatelnou úroveň.
- Sdílení/přenesení rizika – doplněk předcházející možnosti znamená, že v zásadě může správce přesunout vykonání části opatření na jiný subjekt (například zpracovatele) nebo alespoň zajistí pokrytí některých možných následků v případě mimořádných událostí (nelze však postupovat tak, že správci pokryjí rizika pojistnými smlouvami); nicméně správce to nezbavuje odpovědnosti za zpracování osobních údajů (včetně ošetření předpokládaných hrozeb a zranitelností) a případných negativních dopadů na subjekty údajů.
- Akceptace/podstoupení rizika – v některých případech (zejména pokud míra rizika není kritická) může správce riziko akceptovat/podstoupit bez dalších opatření.
- Vyhnutí se riziku – znamená, že správce modifikuje parametry zpracování tak, aby k vysokému nebo kritickému riziku nedocházelo.

V případě snížení a sdílení/přenesení rizika je nutno navrhnout soubor opatření (k řešení rizik, včetně přijatých technických nebo organizačních opatření), jehož cílem je redukce míry rizika na přijatelnou úroveň. Vlastní technická a organizační opatření uplatněná správcem nebo správcem prostřednictvím zpracovatele/dodavatele lze rozdělit na preventivní (realizuje správce na základě posouzení vlivu) a reaktivní/následná po proběhlé mimořádné události (kdy došlo k realizaci hrozby a vzniklo porušení ochrany osobních údajů s tím, že následkem by měla být rovněž revize posouzení vlivu v případě, že lze dopady hodnotit jako střední, vysoké nebo kritické dle Přílohy 5), která mají za cíl zamezit opakování mimořádné události nebo minimalizovat pravděpodobnost jejího opakování.

V případě, že je posouzení rizik prováděno pro více zpracování osobních údajů (například předkladatel právního předpisu, který upravuje totožné zpracování osobních údajů prováděné

řadou subjektů, např. obcí[21]), budou navržená opatření obecnějšího charakteru (důvodem může být skutečnost, že posouzení vlivu nemůže zohledňovat například začlenění zpracování osobních údajů do informačních systémů spravovaných týmž subjektem, např. společné užití podpůrných aktiv). V těchto případech je nutno posouzení vlivu přizpůsobit konkrétním podmínkám správce.

V Příloze 4 jsou uvedeny oblasti, do kterých by měla směřovat přijatá technická a organizační opatření. Jde o obecný seznam a každá položka může být realizována sadou dílčích opatření. Například „detekce, řešení a vyhodnocení mimořádných událostí při zpracování osobních údajů (porušení zabezpečení osobních údajů)“ by mohla být rozdělena na:

- definici odpovědností při řešení mimořádných událostí,
- postupy oznamování mimořádných událostí,
- úpravu spolupráce se zpracovatelem (pokud zpracovatel existuje) při řešení mimořádných událostí,
- postupy klasifikace, šetření a vyhodnocení mimořádných událostí,
- pravidla a postupy revize technických a organizačních opatření na základě mimořádných událostí,
- pravidla vedení evidence a dokumentace mimořádných událostí.

V rámci dalšího postupu (projektu) by měla být technická a organizační opatření dále upřesňována, v případě technických opatření například až na konkrétní SW a HW nástroje, jimiž budou realizována.

6. krok – určení míry rizika po přijetí uvažovaných opatření

V rámci posouzení rizik pro práva a svobody fyzických osob je pro každou hrozbu potřeba uvést, jak se projeví na zpracovávaných osobních údajích a kvantifikovat pomocí hodnocení dopadů, míry hrozeb a míry zranitelností míru rizika pro osobní údaje. Riziko určuje správce postupem dle Přílohy 5, a to po přijetí navrhovaných opatření. Hodnocení míry zranitelnosti, míry hrozby a z toho následně vypočtená míra rizika se bude pohybovat na nižší úrovni (na základě správcem přijatých opatření se snižuje míra zranitelnosti a v některých případech i četnost hrozby). V zásadě může míra rizika pro osobní údaje nabývat hodnot mezi 1 (1x1x1) až 64 (4x4x4). V zásadě by se měla míra rizika pohybovat v rozmezí hodnot 1 až 16. Součástí je určení zbytkových rizik, která správce akceptuje/podstoupí, včetně zdůvodnění jejich přijatelnosti.

(*Poznámka: akceptovatelným zbytkovým rizikem je riziko, které není nutné dále zvládat pomocí dalších bezpečnostních opatření*).

[21] Dle § 62 odstavce 5 zákona č. 110/2019 Sb. u orgánů veřejné moci a veřejných subjektů Úřad pro ochranu osobních údajů musí upustit od uložení správního trestu. Posouzení vlivu na ochranu osobních údajů má tak za účel poskytnout orgánům veřejné moci a veřejným subjektům návod, jak zabezpečit právním předpisem upravené zpracování osobních údajů.

Pokud se nepodaří snížit míru rizika pod hodnotu 48, musí být zahájena předchozí konzultace s Úřadem[22]**.** V rámci konzultace může Úřad správci uložit nápravná opatření[23], včetně zákazu zpracování osobních údajů[24].

4. část – monitorování a aktualizace posouzení vlivu

Po provedení posouzení vlivu je třeba také zajistit monitorování a kontrolovat jeho dodržování.

Monitorovaní a přezkoumávání rizik pro práva a svobody subjektů údajů probíhá soustavně (nová aktiva, nové (dosud neuvažované) hrozby, nové synergické efekty působení hrozeb, identifikace nových zranitelností, po porušení zabezpečení osobních údajů) buď nepřetržitě nebo v plánovaných časových krocích.

Monitorování uplatnění posouzení vlivu, včetně dodržování opatření a revize posouzení vlivu, může být prováděno v rámci mimořádných (po proběhlé mimořádné události, jejímž důsledkem jsou vysoké nebo kritické dopady) nebo plánovaných auditů. V rámci auditu probíhá revize platnosti uvažovaných hrozeb a zranitelností, hodnocení správnosti a účinnosti uplatněných opatření (technických a organizačních), vliv dopadů mimořádných událostí na zpracování osobních údajů, soulad přijatých opatření s právními předpisy a závazky správce a určení případných nápravných opatření. Kontrola uplatnění opatření a aktualizace posouzení vlivu by měly probíhat periodicky v intervalech 1–3 roky s tím, že lze doporučit synchronizaci (z důvodu možnosti duplicity některých prováděných činností) termínu provedení auditu a aktualizace posouzení vlivu s audity kybernetické bezpečnosti prováděnými na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění a vyhlášky č. 82/2018 Sb. (pokud se na správce vztahují). Personální zajištění, koordinace a organizační řešení v případě synchronizace obou auditů je věcí vrcholového vedení příslušného správce.

Monitorování uplatnění posouzení vlivu zajišťuje nezávislá (na monitorovaném zpracování osobních údajů) osoba s odbornými znalostmi a praxí jmenovaná správcem (v případech, kdy se na správce nevztahuje povinnost jmenovat pověřence pro ochranu osobních údajů) nebo pověřenec pro ochranu osobních údajů[25] .

(Poznámka: pověřenec pro ochranu osobních údajů nesmí zpracovávat posouzení vlivu (poskytuje pouze rady a konzultace), protože nemůže poskytovat nezávislý posudek a nezávisle monitorovat posouzení vlivu, které by sám zpracoval).

5. část – stanovisko zástupců subjektů údajů a nezávislých odborníků

Správce zajistí stanovisko subjektů údajů (ve vhodných případech, tj. zejména rozsáhlá zpracování kritických[26] osobních údajů, zpracování údajů umožňujících krádež identity, automatizované rozhodování a případy, kdy budou kladeny vyšší požadavky na spolupráci subjektů údajů z hlediska přijímaných technických a organizačních opatření), ale spíše jen jejich zástupců (vybraný vzorek v rozsahu 3-10 osob) k posouzení vlivu. Subjektům údajů

[22] článek 36
[23] článek 58, odstavec 2
[24] článek 58, odstavec 2, písmeno f)
[25] článek 39, odstavec 1, písmeno c)
[26] viz bod 2.1 v materiálu Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů

nemusí být poskytnut materiál v plném rozsahu, pokud má být zajištěna ochrana obchodních či veřejných zájmů a bezpečnost informací[27]. Posouzení zástupců subjektů údajů může být omezeno na celkové názory a návrhy, zejména na vyjádření:

- k přiměřenosti posuzovaného zpracování osobních údajů (rozsah, předávání, doba uchování, zajištění práv a svobod subjektů údajů),
- k uvažovaným hrozbám,
- k opatřením přijatým správcem, která si vyžadují činnost/spolupráci subjektů údajů.

Pokud správce stanovisko zástupců subjektů údajů nepožaduje, musí to v této části uvést a zdůvodnit. Vyjádření subjektů údajů není třeba, pokud jde o zpracování osobních údajů uložené správci právními předpisy.

Ve vhodných případech (tj. zejména rozsáhlá zpracování kritických[28] osobních údajů, zpracování údajů umožňujících krádež identity, automatizované rozhodování) se doporučuje získat stanovisko nezávislých odborníků různých oborů (právníků, odborníků na informační technologie, odborníků na bezpečnost, ekonomů atd.).

Správce doplní vyjádření výše uvedených subjektů o vypořádání, ve kterém uvede, které návrhy neakceptoval a proč.

6. část – posudek pověřence pro ochranu osobních údajů

Vyjádření pověřence pro ochranu osobních údajů obsahuje výroky o:

- přiměřenosti rozsahu, parametrů zpracování osobních údajů a zákonnosti zpracování,
- úplnosti posouzení vlivu,
- přiměřenosti přijatých opatření (technických a organizačních),
- nutnosti provedení předchozí konzultace[29] s Úřadem (jen pokud míra rizika zůstává i po posouzení vlivu na úrovni kritická).

7. část – předchozí konzultace s Úřadem

Pokud se nepodaří snížit míru rizika pod hodnotu 48, musí být zahájena předchozí konzultace s Úřadem[29]. V rámci předchozí konzultace může Úřad využít vůči správci některou z nápravných pravomocí dle čl. 58 nařízení (a to včetně zákazu zpracování osobních údajů[30]). Dokumentace výsledku předchozí konzultace s Úřadem je součástí posouzení vlivu.

8. část – doložka o schválení posouzení vlivu odpovědnou osobou správce

Na závěr posouzení vlivu je připojena doložka o schválení odpovědnou osobou správce (nejčastěji statutární zástupce správce) obsahující alespoň identifikaci schvalovaného posouzení vlivu, schvalovací text, datum schválení a podpis statutárního zástupce.

[27] článek 35, odstavec 9
[28] článek 35, odstavec 3, písmeno b)
[29] článek 36, odstavec 1
[30] článek 58, odstavec 2, písmeno f)

4. etapa

Monitorování dodržování opatření a pravidelné revize posouzení vlivu

Soustavné monitorování a pravidelné přezkoumávání rizik pro práva a svobody subjektů údajů (probíhá před začleněním nových aktiv do zpracování, vznikem nových (dosud neuvažovaných) hrozeb, vznikem nových synergických efektů působení hrozeb, identifikací nových zranitelností, po porušení zabezpečení osobních údajů). Využít lze například některých nástrojů pro monitorování zpracování osobních údajů, varování a informací vydávaných CERT/CSIRT apod.

Audit dodržování opatření dle přijatého harmonogramu (nebo mimořádný).

Provádění revizí posouzení vlivu dle přijatého harmonogramu.

Použitá literatura:

WP248 rev. 1 Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679

Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů DPIA (zde)

Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (zde)

ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací

ČSN EN ISO/IEC 27001 Informační technologie – Systém řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací

ČSN ISO/IEC 29151 Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací

ČSN ISO/IEC 27018 Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

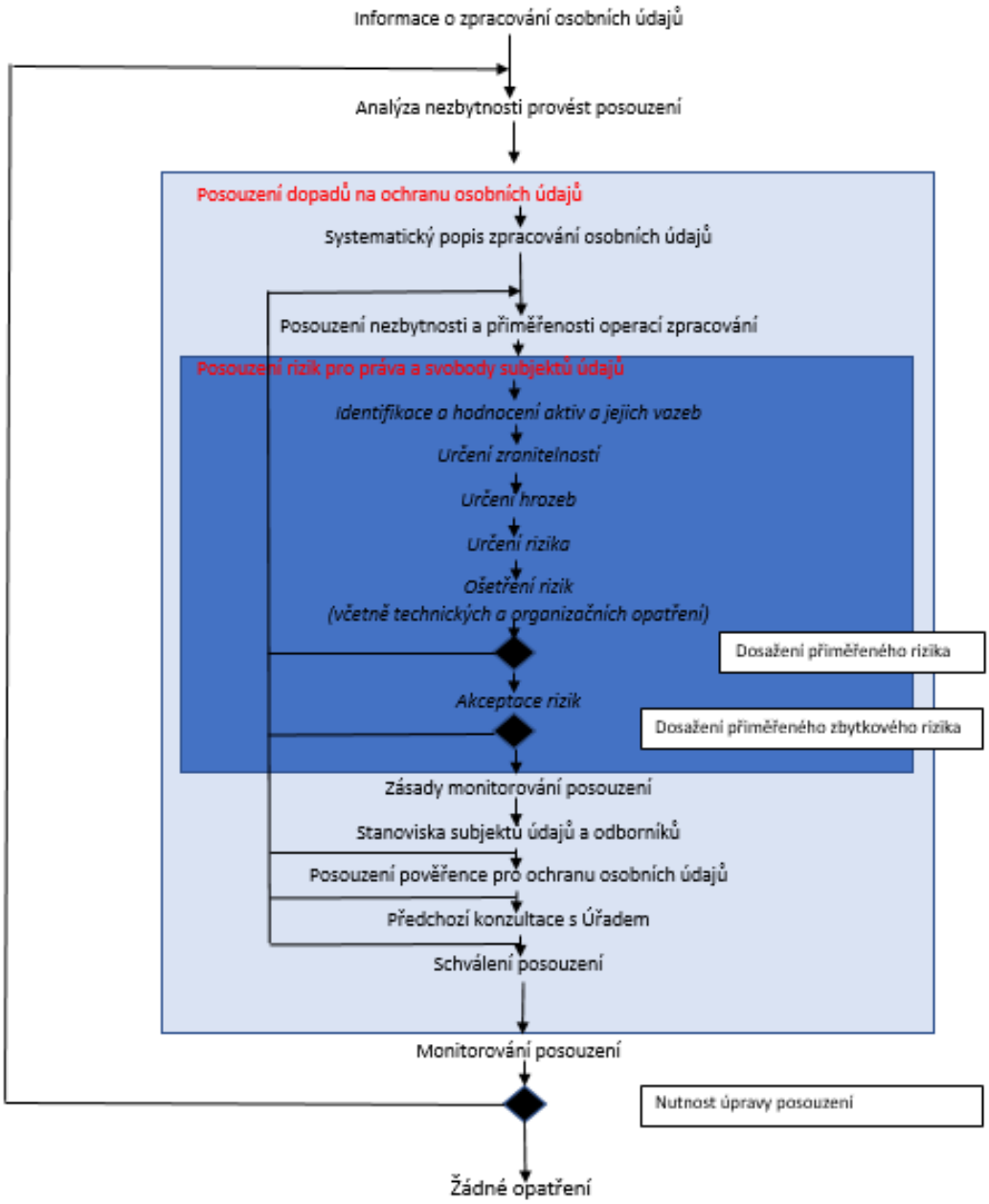
ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

ČSN ISO/IEC 29134 Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu do soukromí

ČSN ISO 31000 Management rizik – Principy a směrnice

Příloha 1

Postup správce při provádění posouzení vlivu – schéma



Příloha 2

Příklady zranitelností

- zastaralost informačních a komunikačních technologií podporujících zpracování osobních údajů;
- nedostatečná údržba informačních a komunikačních technologií podporujících zpracování osobních údajů;
- nedostatečná fyzická ochrana míst zpracování osobních údajů;
- nedostatečné povědomí určených osob o postupech zpracování a zabezpečení osobních údajů;
- nedostatečné řízení přístupu k osobním údajům;
- nedostatečné postupy při identifikování a odhalení mimořádných událostí a nebezpečných jevů;
- nedostatečné monitorování činnosti, neschopnost odhalit nežádoucí způsoby chování nebo pochybení určených osob;
- nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností a bezpečnostních rolí v rámci zpracování osobních údajů;
- nedostatečná ochrana aktiv;
- nevhodná bezpečnostní architektura;
- nedostatečná (nezávislá) kontrola apod.

(Poznámka: některé detailnější nebo modifikované informace k určení zranitelnosti lze nalézt v ČSN ISO/IEC 27005 a vyhlášce č. 82/2018 Sb.).

Příloha 3

Příklady hrozeb

- poškození nebo selhání technického anebo programového vybavení (HW, SW, nosiče osobních údajů);
- neoprávněný přístup k osobním údajům (zneužití nebo odcizení identity interními nebo externími osobami);
- zavedení škodlivého kódu (například viry, spyware, trojské koně);
- narušení fyzické bezpečnosti;
- přerušení poskytování služeb elektronických komunikací nebo dalších komunikačních služeb (doručování) nezbytných pro zpracování osobních údajů;
- zneužití nebo neoprávněná modifikace údajů (použití osobních údajů k účelu, který není deklarován, popření provedení akce s osobními údaji, vyzrazení osobních údajů);
- ztráta, odcizení nebo poškození aktiva s osobními údaji;
- nesprávné řízení ochrany osobních údajů (nedodržení smluvního závazku ze strany dodavatele, nedodržení právních předpisů, užívání programového vybavení v rozporu s licenčními podmínkami);
- pochybení ze strany určených osob (uživatelé, zaměstnanci, administrátoři, operátoři údržby);
- zneužití vnitřních prostředků (nenormální použití aktiv – použití pro osobní účely, instalace neschválených programů);
- úmyslné poškození (poškození kabeláže, fyzické napadení osoby, krádež pošty, cílený teroristický útok apod.);
- selhání prostředí (přírodní katastrofy, technická selhání, tj. poruchy nebo výpadky dodávek vody, elektřiny, klimatizace, necílený teroristický útok);
- nedostatek zaměstnanců s potřebnou odbornou úrovní;
- sociální inženýrství;
- špionážní techniky (určování polohy, odposlech, sledování obsahu obrazovky, čtení, pořizování fotokopií, fotografování);
- zneužití vyměnitelných technických a jiných nosičů dat (kopírování osobních údajů z nosičů dat, vyzrazení informací z vyřazeného, nedostatečně vymazaného média);
- napadení komunikace (odposlech, modifikace, šíření cizího kódu) apod.

(Poznámka: některé detailnější nebo modifikované hrozby lze nalézt v ČSN ISO/IEC 27005, ČSN ISO/IEC 29134 a vyhlášce č. 82/2018 Sb.).

Příloha 4

Příklady zaměření technických a organizačních opatření

Technická opatření směřují k:

- zajištění fyzické bezpečnosti míst zpracování osobních údajů (řízení fyzického přístupu do prostor/objektu, ochrana perimetru míst zpracování osobních údajů);
- zabezpečení práce s mobilními zařízeními a vzdálené práce;
- zabezpečení komunikačního prostředí/sítí;
- správě a ověřování identity určených osob;
- řízení přístupových oprávnění;
- monitorování a zaznamenávání činnosti určených osob;
- detekci, řešení a vyhodnocení mimořádných událostí při zpracování osobních údajů (porušení zabezpečení osobních údajů);
- ochraně před škodlivými kódy;
- ochraně identity subjektů údajů (pseudonymizace, anonymizace osobních údajů);
- zajištění čitelnosti osobních údajů pouze oprávněnými osobami (kryptografie);
- zajištění požadované úrovně dostupnosti osobních údajů;
- zajištění zálohování a archivace;
- zajištění aplikační bezpečnosti apod.

Organizační opatření směřují k:

- zajištění systému řízení ochrany osobních údajů;
- zajištění řízení aktiv;
- zajištění řízení rizik;
- klasifikaci osobních údajů;
- řízení dodavatelů/zpracovatelů (včetně dodavatelů digitálních služeb);
- organizačnímu zajištění zpracování osobních údajů;
- bezpečnosti lidských zdrojů;
- řízení přístupu;
- zajištění požadované dokumentace zpracování osobních údajů;
- zajištění bezpečnosti v procesech akvizice, vývoje a údržby;
- řízení změn;
- řízení provozu a komunikací;
- řízení kontinuity činností;
- řízení monitorování zpracování osobních údajů a revize posouzení vlivu apod.

(Poznámka: některé podrobnější informace k opatřením lze nalézt v ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, ČSN ISO/IEC 29151, ČSN ISO/IEC 27018 a vyhlášce č. 82/2018 Sb.).

Příloha 5

Provádění posouzení rizik pro práva a svobody fyzických osob

V rámci posouzení vlivu je pro každou hrozbu (která působí na určené aktivum prostřednictvím určené zranitelnosti) nutno uvést, jaký je její vliv na osobní údaje (narušení dostupnosti, integrity nebo důvěrnosti) a kvantifikovat (pomocí hodnocení závažnosti události, míry hrozby, a míry zranitelnosti) míru rizika pro osobní údaje. Níže v příloze je uveden způsob, jak toho docílit.

- Vliv realizace hrozby na osobní údaje
  Pro každou hrozbu se označí zaškrtnutím jeden nebo i více vlivů (nepřiděluje se hodnota)
  - Ztráta integrity osobních údajů (neoprávněné pozměnění osobních údajů),
  - Ztráta dostupnosti osobních údajů (zničení, krádež, neoprávněné odstranění, ztráta osobních údajů),
  - Ztráta důvěrnosti osobních údajů (neoprávněné zpřístupnění osobních údajů).

- Dopady – hodnocení závažnosti události
  Definuje se pomocí hodnoty vyjadřující závažnost (rozsah a hloubku) dopadů pro subjekty údajů a pro správce, což ve výsledku komplexně řeší problém vyhodnocení realizace hrozeb. Hodnocení dopadů probíhá v závislosti na zpracovávaných osobních údajích (identifikace subjektu údajů, citlivost informací), druhu a rozsahu újmy způsobené fyzickým osobám a správci. V případě hodnocení dopadů na fyzickou újmu se nepředpokládá účast znalců (např. lékařů) na určení její míry. Jako výsledná hodnota je brána nejvyšší dosažená úroveň.

Dopady		Dopady na subjekty údajů	Finanční újma subjektů údajů	Finanční náklady správce	Narušení běžných činností správce	Ztráta důvěryhodnosti správce	Dopad na zaměstnance správce	Mezinárodní vztahy (předávání)
1	**Nízké**	Může vést k nepohodlí subjektu údajů (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace se správcem).	Finanční újma nehrozí.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu správce,	K narušení běžných činností nedochází, nanejvýše ke zvýšeným časovým nárokům při zpracování osobních údajů.	Může negativně ovlivnit vztahy s jinými částmi správce, jinými subjekty nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání (nepříjemnosti se subjekty údajů, nutnost jednání s dalšími subjekty, negativní, někdy i veřejné, reakce subjektů údajů apod.).	Může způsobit krátkodobé nepříjemnosti při zpracování osobních údajů (zdržení a podráždění zaměstnanců nebo členů správce, jiné zdravotní dopady nehrozí).	Může vyvolat nutnost jednání mezi správcem a zahraničním partnerem o charakteristikách zpracování osobních údajů.

2	**Střední**	Může vést k menší újmě (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke službám správce nebo jiných subjektů, časové nároky spojené s řešením dopadů).	Odhadovaná finanční újma do 5000 Kč/subjekt údajů.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu správce	Může omezit provádění běžných činností, narušit řádné řízení nebo fungování části nebo celého správce, krátkodobý výpadek služeb správce.	Může negativně ovlivnit vztahy s jinými subjekty nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá (úbytek subjektů údajů do 10 % u správce, krátkodobé omezení přístupu ke službám využívaným správcem, negativní, avšak krátkodobé ohlasy v médiích).	Může negativně ovlivnit výkon zaměstnanců při zpracování osobních údajů (stres zaměstnanců a členů správce, drobné fyzické a zdravotní obtíže).	Může docházet k vytváření negativního obrazu správce u zahraničních partnerů v jednom teritoriu, popř. v jednom státě, vedoucího k dočasnému omezení zahraniční participace na zpracování osobních údajů.
3	**Vysoké**	Může vést k závažné újmě (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány).	Odhadovaná finanční újma od 5000 Kč do 50000 Kč/ subjekt údajů, (zneužití finančních prostředků subjektu údajů, poškození majetku).	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu správce.	Může způsobit dočasné zastavení nebo podstatné narušení běžných činností správce nebo poškodit rozvoj nebo prosazování cílů a zájmů správce.	Může závažně ovlivnit vztahy s jinými subjekty nebo veřejností s následkem celostátní negativní publicity (úbytek subjektů údajů 10-50 % u správce, dlouhodobé omezení nebo zamezení přístupu ke službám využívaným správcem, masivní, negativní, avšak krátkodobé ohlasy v médiích).	Může způsobit závažné, krátkodobé omezení výkonu při zpracování osobních údajů (zhoršení zdravotního stavu zaměstnanců členů, krátkodobá pracovní neschopnost).	Může docházet k vytváření negativního obrazu správce u zahraničních partnerů a veřejnosti ve světě, spojeného s trvalým nebo dlouhodobým omezením participace zahraničních partnerů na zpracování osobních údajů.
4	**Kritické**	Může vést k velmi závažné újmě, přímému ohrožení či ztrátě života (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).	Odhadovaná finanční újma od 50000 Kč/ subjekt údajů (neschopnost splácet dluh, ztráta majetku).	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace správce.	Může závažně a dlouhodobě ovlivnit vztahy s jinými subjekty nebo veřejností s následkem celostátní negativní publicity, s dlouhodobými účinky a újmou (soudní proces, likvidace, vznik nesplatitelného dluhu apod.)	Může závažně a dlouhodobě ovlivnit vztahy s jinými subjekty nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky na přijetí odpovědnosti (úbytek subjektů údajů nad 50 % u správce, černé listiny, ztráta konkurenceschopnosti, masivní, negativní, dlouhodobé ohlasy v médiích, včetně zahraničních).	Může způsobit závažné dlouhodobé omezení výkonu při zpracování osobních údajů (útoky na členy nebo zaměstnance společnosti, odchod zaměstnanců nebo členů, dlouhodobá pracovní neschopnost, úmrtí).	Může docházet k vytváření negativního obrazu České republiky v oblasti zpracování a ochrany osobních údajů po celém světě, spojeného s dlouhodobým nebo trvalým omezením participace zahraničních subjektů nebo i států na zpracování osobních údajů.

- Míra hrozby – míra pravděpodobnosti výskytu hrozby
  Definuje se pomocí hodnoty vyjadřující četnost výskytu hrozeb.

Míra hrozby		Popis
1	Nízká	Frekvence výskytu hrozby není častější než jednou za pět let.
2	Střední	Frekvence výskytu hrozeb se pohybuje v rozpětí od jednoho roku do pěti let.
3	Vysoká	Frekvence výskytu hrozeb se pohybuje rozpětí od jednoho měsíce do jednoho roku.
4	Kritická	Frekvence výskytu hrozeb se pohybuje v častějších intervalech než jednou za měsíc.

- Míra zranitelnosti (zranitelnost)
  Definuje se pomocí hodnoty vyjadřující využití zranitelnosti na základě přijatých opatření

Míra zranitelnosti		Popis
1	Nízká	Využití zranitelnosti se nejeví jako možné. Existují opatření, která jsou schopna včas detekovat pokusy o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům (úspěšné pokusy nejsou známy) o narušení integrity, dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
2	Střední	Využití zranitelnosti se jeví jako obtížné. Existují opatření, která jsou jen omezeně schopna včas detekovat pokusy o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům (úspěšné pokusy nejsou známy) o narušení integrity, dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
3	Vysoká	Využití zranitelnosti se jeví jako možné. Neexistuje detekce pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů; přijatá opatření jsou schopna zamezit pokusům o narušení integrity, dostupnosti a důvěrnosti osobních údajů jen omezeně (jsou známy dílčí úspěšné pokusy); účinnost opatření není kontrolována; opatření nejsou pravidelně revidována.
4	Kritická	Využití zranitelnosti se jeví jako snadné. Neexistuje detekce pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů; nejsou přijata opatření k zamezení pokusů o narušení integrity, dostupnosti a důvěrnosti osobních údajů nebo je jejich účinnost velmi omezená (jsou známy úspěšné pokusy); účinnost opatření (pokud jsou nějaká přijata) není kontrolována; opatření (pokud jsou přijata) nejsou revidována.

- Určení míry rizika pro osobní údaje

Na základě stanovených koeficientů pro hodnocení dopadů, hrozeb a zranitelností se vypočte míra rizika. K tomu lze použít následující vzorec.

riziko = dopad x míra hrozby x míra zranitelnosti

Obecně tedy může míra rizika pro osobní údaje nabývat hodnot mezi 1-64. Výsledné hodnoty lze rozdělit do několika skupin dle jeho úrovně.

- **Riziko nízké** (hodnoty 1-4) – riziko je považováno za přijatelné (riziko akceptováno automaticky).
- **Riziko střední** (hodnoty 6-16) – riziko je vhodné snížit finančně méně nákladnými opatřeními, to znamená, že je možné riziko akceptovat, pokud by možná opatření byla nepřiměřeně nákladná (riziko akceptuje DPO).
- **Riziko vysoké** (hodnoty 18-36) – riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění (riziko krátkodobě akceptuje DPO).
- **Riziko kritické** (hodnoty 48-64) – riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho eliminaci (považováno za vysoké riziko ve smyslu článku 36 odstavec 1).

Posouzení rizik (část 3 zpracování posouzení) lze zpracovat v tabulce, kde se v jednotlivých sloupcích uvede: aktivum (podpůrné aktivum); zranitelnost; hrozba; vliv realizace hrozby se sloupci (ztráta) integrity, dostupnosti, důvěrnosti; rizika před přijetím opatření se sloupci dopady, hrozby, zranitelnosti, riziko; přijatá opatření (uvede se číslo opatření ze seznamu zpracovaného správcem); rizika po přijetí opatření se sloupci dopady, hrozby, zranitelnost, zbytkové riziko. Tato tabulka ukazuje pouze výslednou, **přehlednou a formální** úpravu, nečiní si ambici ukázat nějaké vzorové řešení. Řešení provádí samostatně každý správce se znalostí hodnoceného zpracování osobních údajů. Je zřejmé, že určení hodnoty u dopadů, zranitelností a hrozeb musí předcházet analýza za účasti správcem určených odborníků, nejde o pouhé formální vyplnění tabulky (viz následující strana).

Příklad tabulky pro posouzení rizik

Aktivum	Zranitelnost	Hrozba	Vliv hrozby na OÚ			Riziko před přijetím opatření			
			ztráta integrity	ztráta dostupnosti	ztráta důvěrnosti	dopady	míra hrozby	míra zranitelnost	riziko
aplikace	Nedostatečné řízení přístupu k OÚ	Zneužití nebo neoprávněná modifikace OÚ	x		x	3	3	4	36
server	Nedostatečná údržba ICT	Poškození nebo selhání technického vybavení		x		2	2	4	16
atd.									

Přijatá opatření	Riziko po přijetí opatření			
	dopady	míra hrozby	míra zranitelnosti	zbytkové riziko
1, 2*)	3	3	1	9
3, 4*)	2	2	1	4

Poznámka:

*) číslo opatření ze seznamu technických a organizačních opatření připraveného správcem např. 1 – správa řízení identity, 2 – řízení přístupu, 3 – řízení aktiv, 4 – zálohování a archivace dat (navazuje na etapu 3, krok 5 tohoto materiálu)