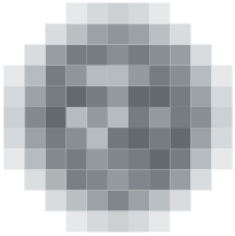
Metodika obecného posouzení vlivu na ochranu osobních údajů

23. října 2019

Verze 0.6

(návrh dokumentu určený k veřejné diskuzi, dokument určený pro přímé využití bude ve verzi 1.0)



úřad pro ochranu osobních údajů
the office for personal data protection

úřad pro ochranu osobních údajů
the office for personal data protection

Obsah:

úřad pro ochranu osobních údajů
the office for personal data protection

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 nařízení) předpokládá v některých případech (článek 35) vypracování 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 připravena s ohledem 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),
- další odborné podklady/dokumenty, které jsou k uvedené problematice k dispozici.

Je třeba upozornit na to, že pro posouzení vlivu u 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 na základě § 10 zákona o zpracování osobních údajů se tento dokument použije jako výchozí. Úřad vypracoval návod k posouzení vlivu u návrhů právních předpisů,[6] který stanoví specifika pro tuto oblast a je v současné době předmětem revize.

Metodika je 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 (v současnosti předkládané legislativní návrhy většinou neobsahují konkrétní posouzení rizik pro práva a svobody subjektů údajů a plánovaná opatření k řešení těchto rizik) i další odborníci na ochranu osobních údajů.

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

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

úřad pro ochranu osobních údajů
the office for personal data protection

K provádění posouzení vlivu v otázkách a odpovědích

Správci při přípravě zpracování osobních údajů budou řešit problémy souvisejí 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**.

Posouzení vlivu se zpravidla připravuje pro (operace) zpracování osobních údajů (jeho hranice definuje správce – například to může být účetnictví, 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 zpracovávat 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).

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

- 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 zpracovat 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:

- změnami parametrů zpracování,
- použitím nových technologií,
- změnami právních předpisů,
- expanzí správce (územní nebo organizační)
- vznikem nových/neznámých hrozeb pro zpracování 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.

Po posouzení vlivu by dodržování přijatých opatření mělo být pravidelně monitorováno a periodicky prověřováno v závislosti na změně rizika[14] nebo proběhlých mimořádných událostech, tj. porušení zabezpečení osobních údajů[15]. K tomu Pokyny WP 248 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 údajů v postupně se měnícím prostředí.

[11] článek 35, odstavec 10, recitál bod 92
[12] článek 35, odstavec 8
[13] článek 26
[14] článek 35, odstavec 11
[15] článek 33 odstavec 3, písmeno d

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.

5) Jak se posouzení vlivu provádí?

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

1.etapa – shromáždění informací o zpracování osobních údajů.

2.etapa – analýza (na základě informací dle předchozí odrážky), zda je povinné zpracovávat posouzení vlivu.

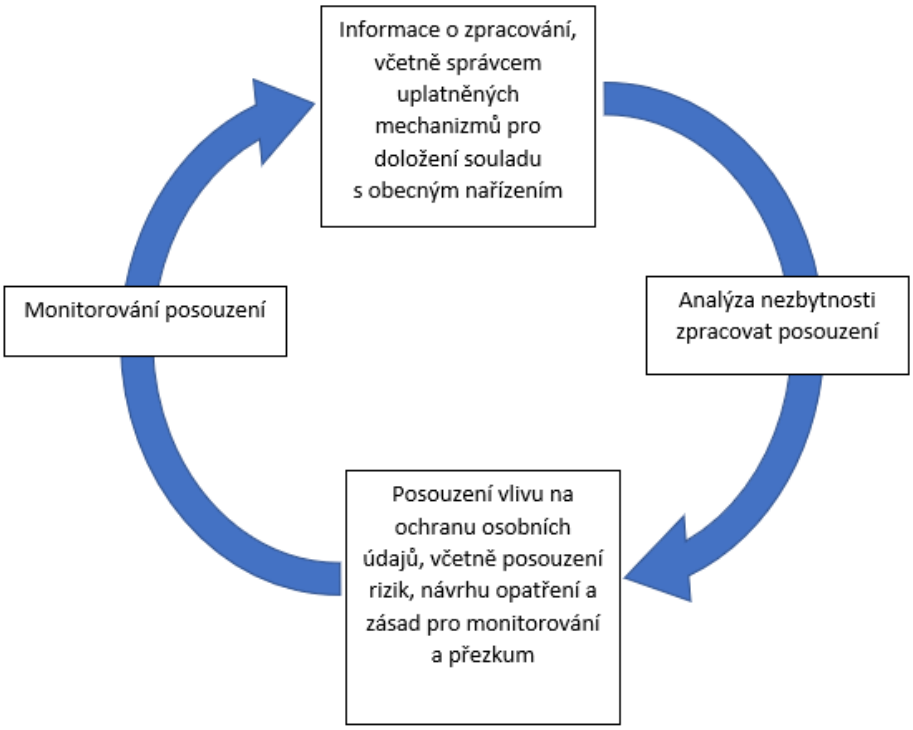
3.etapa – vlastní posouzení vlivu.

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

[16] článek 24, odstavec 1
[17] článek 35, odstavec 7

Zpracování 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 zpracovat posouzení vlivu. Podrobný rozpis postupu je uveden v Příloze 1.



Obr. 1 Schéma postupu správce

1. etapa
shromáždění informací o zpracování osobních údajů

Pro provedení analýzy, zda je správce povinen zpracovat posouzení vlivu, je nezbytné mít k dispozici určité údaje o zpracování osobních údajů. Postačují informace v rozsahu – popis vlastního zpracování, účel/ly zpracování osobních údajů, 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[18], které musí každý správce vést (pokud neprovádí nahodilá zpracování osobních údajů).

[18] článek 30

2. etapa
analýza, zda je povinné zpracovávat posouzení vlivu

Povinnost zpracovávat 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:

1. **krok** – nahlédnutí seznamu druhů operací, které nepodléhají posouzení vlivu, který Úřad připravil a je k dispozici **zde**[19]. 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, které nepodléhají vlivu na ochranu osobních údajů), potom by měl provést analýzu zpracování osobních údajů na základě parametrů jím prováděného zpracování osobních údajů a seznamu operací (seznam je zpracován jako parametrický), které podléhají požadavku posouzení vlivu a který Úřad připravil a je k dispozici **zde**. Seznam podléhá schválení Evropským sborem pro ochranu osobních údajů a může zaznamenat určité změny.

3. etapa
vypracování posouzení vlivu

Vlastní posouzení vlivu lze rozdělit do osmi částí, ve kterých správce provádí řadu kroků.

1. část – systematický popis zamýšlených operací zpracování

- název a identifikace správce/sdílených správců,
- název a krátký popis (operací) zpracování osobních údajů,
- 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 určená zákonem, musí být uvedeno, který zákon a který § povinnost ukládá),
- seznam zpracovávaných údajů (zde asi nepostačují pro provedení analýzy kategorie osobních údajů),
- předpokládaná doba uchování osobních údajů,
- popis subjektů údajů (zde by postačoval údaj na úrovni kategorie, například – zaměstnanci, studenti, příjemci dávek, pacienti apod.),
- popis 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 apod.),
- popis zajištění práv a povinností subjektů údajů,
- diagram (workflow) popisující zpracování (tok) osobních údajů.

[19] Seznam je ve stavu posuzování v rámci struktur Evropského sboru pro ochranu osobních údajů, po schválení bude hypertextový odkaz vložen.

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 seznam hrozeb pro dané zpracování údajů a také seznam opatření, jak tyto hrozby eliminovat. To by, při oddělené analýze, mohlo vést k určitým nekonzistentnostem z hlediska přijatých opatření.

1. krok – identifikace primárních aktiv (zajišťované procesy a činnosti, zpracovávané informace) a sekundárních/podpůrných aktiv (HW, SW, sítě, nosiče informací, pracovníci, lokality, organizace)

2. krok – určení zranitelností

identifikují se zranitelnosti, prostřednictvím jichž jsou realizovány hrozby, jako jsou:

- 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.

3. krok – určení hrozeb

s ohledem na aktiva správce identifikuje relevantní hrozby, jako jsou:

- 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.

4. krok – určení rizika před přijetím jakýchkoliv opatření

V rámci posouzení rizik pro práva a svobody fyzických osob pro každou hrozbu uvést, jak se projeví na zpracovávaných osobních údajích a kvantifikovat pomocí hodnocení dopadů, míry hrozeb a míry zranitelností míru rizika pro osobní údaje. Míru rizika určuje správce postupem dle přílohy 2, a to před jeho redukcí (propočet probíhá s tím, že hodnocení míry zranitelnosti bude mít vždy hodnotu 4). V rámci tohoto přístupu lze určit hrozby, které mají vysokou míru rizika a vyžadují další zásahy (redukci míry rizika např. prostřednictvím technických a organizačních opatření). V zásadě může míra rizika u jednotlivých hrozeb pro osobní údaje nabývat hodnot mezi 6 (1+1+4) až 12 (4+4+4).

5. krok – ošetření rizik (způsob řešení rizik a přijetí opatření k řešení rizik).

Z posouzení vlivu vyjde u některých hrozeb riziko jako kritické, vysoké nebo střední. Možností redukce rizika pro osobní údaje je několik.

- Modifikace rizika – přijetí opatření na straně správce, tak aby míra rizika byl snížena na přijatelnou úroveň.
- Sdílení rizika – doplněk předcházející možnosti znamená, že v zásadě může správce přesunout vykonání části opatření na třetí stranu (například zpracovatele) nebo alespoň zajistí pokrytí některých následků v případě mimořádných událostí (nelze však postupovat tak, že správci pokryjí rizika

pojistnými smlouvami); nicméně správce to nezbavuje odpovědnosti za zpracování osobních údajů a případných dopadů na subjekty údajů.

- Podstoupení rizika – v některých případech (zejména pokud míra rizika není kritická) může správce riziko podstoupit bez dalších opatření.
- Vyhnutí se riziku – znamená, že správce modifikuje parametry zpracování tak, aby k riziku nedocházelo nebo bylo sníženo na přijatelnou míru (riziko nízké nebo střední).

V případě modifikace a sdílení rizika je nutno navrhnout soubor opatření (k řešení rizik, včetně přijatých technických nebo organizačních opatření), jehož cílem je redukce 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, významné nebo kritické), která mají za cíl zamezit opakování mimořádné události nebo minimalizovat pravděpodobnost jejího opakování.

Technická opatření směřují k:

- zajištění fyzické bezpečnosti míst zpracování osobních údajů (řízení fyzického přístupu do prostor/objektu, ochrana perimetru míst zpracování osobních údajů);
- 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;
- řízení dodavatelů (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 a vyhlášce č. 82/2018 Sb.

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), budou navržená opatření obecnějšího charakteru (posouzení totiž 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 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 rizika po přijetí uvažovaných opatření
V rámci posouzení rizik pro práva a svobody fyzických osob pro každou hrozbu 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 2, a to po přijetí opatření. Hodnocení míry zranitelnosti může nabývat koeficientu 1 až 4 a ke změnám může dojít i při hodnocení dopadů a míry hrozby, a to v závislosti na předchozím kroku (tedy včetně technických a organizačních opatření přijatých správcem). V zásadě může míra rizika pro osobní údaje nabývat hodnot mezi 3 (1+1+1) až 12 (4+4+4). Ve skutečnosti by se v zásadě měla rizika u jednotlivých hrozeb pohybovat v rozmezí hodnot 3 až 7. Součástí je určení zbytkových rizik, která správce podstoupí, včetně zdůvodnění jejich přijatelnosti.
(*Poznámka: akceptovatelným zbytkovým rizikem je riziko, které je přijatelné a není nutné jej zvládat pomocí dalších bezpečnostních opatření*).

Pokud se nepodaří u některé hrozby snížit riziko pod hodnotu 11, musí být zahájena předchozí konzultace s Úřadem[20]. V rámci konzultace může Úřad správci uložit nápravná opatření[21], včetně zákazu zpracování osobních údajů[22].

4. část – monitorování a aktualizace posouzení vlivu
Po zpracování posouzení vlivu je třeba také zajistit monitorování a kontrolovat jeho dodržování.
Monitorovaní a přezkoumávání rizik pro práva a svobody subjektů údajů probíhá nepřetržitě (nová aktiva, nové (dosud neuvažované) hrozby, nové synergické efekty působení hrozeb, identifikace nových zranitelností, po porušení zabezpečení osobních údajů).
Monitorování uplatnění posouzení vlivu, včetně dodržování opatření a revize posouzení vlivu, může být prováděna v rámci mimořádných (po proběhlé mimořádné události, jejímž důsledkem jsou významné nebo kritické dopady) nebo plánovaných auditů. V rámci auditu probíhá revize platnosti uvažovaných hrozeb, 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

[20] článek 36
[21] článek 58, odstavec 2
[22] článek 58, odstavec 2, písmeno f

by měla probíhat periodicky v intervalech 1–3 roky s tím, že lze doporučit synchronizaci 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 (pokud se na správce vztahují).
Monitorování uplatnění posouzení vlivu zajišťuje nezávislá 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[23] .
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, který by sám zpracoval.

5. část – stanovisko zástupců subjektů údajů a nezávislých odborníků

Správce zajistí stanovisko uživatelů (ve vhodných případech, tj. zejména rozsáhlá zpracování speciálních kategorií 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 nemusí být poskytnut materiál v plném rozsahu, pokud má být zajištěna ochrana obchodních či veřejných zájmů a bezpečnost informací[24]. 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, která by měl přijmout subjekt údajů.

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

Ve vhodných případech (tj. zejména rozsáhlá zpracování speciálních kategorií 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 a parametrů zpracování osobních údajů,
- úplnosti posouzení vlivu,
- přiměřenosti přijatých opatření (technických a organizačních),
- nutnosti provedení předchozí konzultace[20] s Úřadem (jen pokud míra rizika zůstává i po posouzení vlivu na úrovni kritická).

[23] článek 39, odstavec 1, písmeno c
[24] článek 35, odstavec 9

7. část – předchozí konzultace s Úřadem

Pokud se nepodaří u některé hrozby snížit míru rizika pod hodnotu 11, musí být zahájena předchozí konzultace s Úřadem[20]. V rámci předchozí konzultace může Úřad využít vůči správci některou z nápravných pravomocí (a to včetně zákazu zpracování osobních údajů)[22].
Rozhodnutí vydané Úřadem je součástí posouzení vlivu.

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

4. etapa
monitorování dodržování opatření a pravidelné revize posouzení vlivu

Nepřetržité monitorování a přezkoumávání rizik pro práva a svobody subjektů údajů.
Audit dle přijatého harmonogramu (nebo mimořádný).
Provádění revizí posouzení vlivu dle přijatého harmonogramu.

úřad pro ochranu osobních údajů
the office for personal data protection

Použitá literatura:

1) 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 (obecné nařízení o ochraně osobních údajů).

2) 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.

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

4) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (zrušen)

5) Zákon č. 110/2019 Sb., o zpracování osobních údajů

6) Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

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

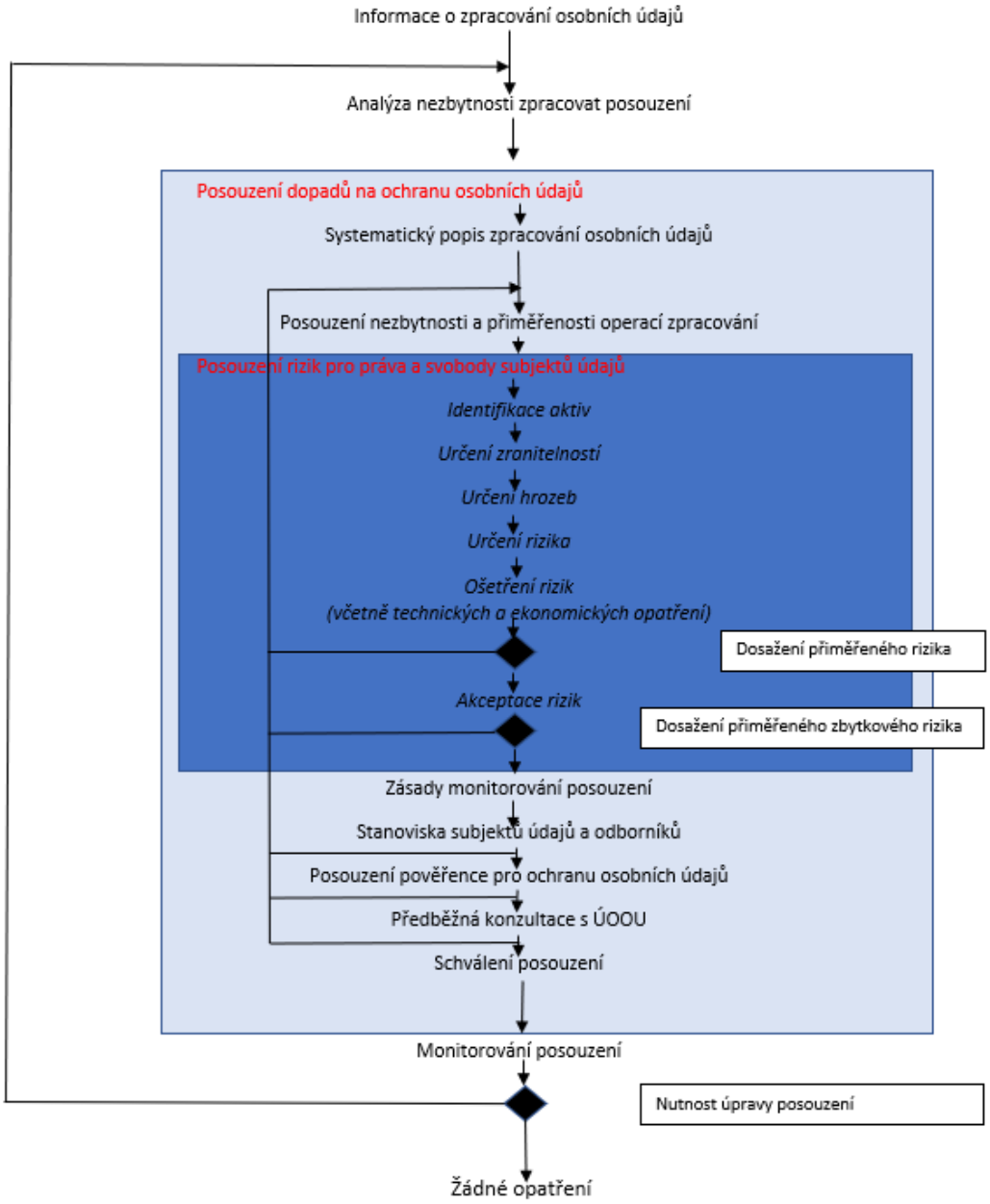
8) ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.

9) ČSN ISO/IEC 27001 Informační technologie – Systém řízení bezpečnosti informací – Požadavky.

10) ČSN ISO 31000 Management rizik – Principy a směrnice.

Příloha 1

Postup správce při provádění posouzení vlivu



úřad pro ochranu osobních údajů
the office for personal data protection

Příloha 2

Posuzování rizik pro práva a svobody fyzických osob

V rámci posouzení vlivu je třeba pro každou hrozbu uvést, jak se projeví na zpracovávaných osobních údajích a kvantifikovat pomocí hodnocení dopadů, míry hrozeb a míry zranitelností míru rizika pro osobní údaje. Zde je návrh způsobu, jak toho lze 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 – závažnost události**
  Definuje se pomocí hodnoty vyjadřující závažnost (rozsah a hloubku) dopadů pro subjekty údajů a pro správce. Hodnocení dopadů je v závislosti na zpracovávaných údajích (identifikace subjektu, citlivost), druhu a rozsahu újmy způsobené fyzickým osobám a správci.
  - Zanedbatelné dopady (koeficient 1)
    Nevýznamné dopady, které lze překonat bez obtíží.
    Pro správce – fyzická újma (podráždění zaměstnanců, jiné zdravotní dopady nehrozí), společenské (nepříjemnosti se subjekty údajů, nutnost jednání s dalšími subjekty), finanční náklady do 50 000 Kč apod.
    Pro subjekty údajů – fyzická újma (podrážděnost, nepohodlí), společenské (krátkodobé časové nároky pro opětovné zadávání údajů, komunikace se správcem), finanční újma nehrozí apod.
  - Omezené dopady (koeficient 2)
    Dopady, které lze překonat s určitými obtížemi.
    Pro správce – fyzická újma (stres zaměstnanců, drobné fyzické obtíže), společenské (krátkodobé omezení přístupu ke službám využívaným správcem, krátkodobý výpadek služeb správce), finanční náklady od 50 000 do 500 000 Kč apod.
    Pro subjekty údajů – fyzická újma (stres, nepohodlí, podráždění, drobné fyzické obtíže), společenské (nedostatek porozumění, omezení přístupu ke službám správce, časové nároky spojené s řešením dopadů), finanční újma (do 5000 Kč/osoba) apod.
  - Významné dopady (koeficient 3)
    Dopady, které lze překonat jen s velkými obtížemi.
    Pro správce – fyzická újma (zhoršení zdravotního stavu zaměstnanců), společenská (černé listiny, ztráty pověsti, ztráty zaměstnání, ztráta konkurenceschopnosti, předvolání vyšetřujícími orgány), finanční náklady od 500 000 do 5 000 000 Kč apod.
    Pro subjekty údajů – fyzická újma (napadení, nepříznivý zdravotní stav, deprese), společenské (ztráta zaměstnání, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež

identity, předvolání vyšetřujícími orgány), finanční újma (zneužití finančních prostředků, dodatečné náklady, poškození majetku, škoda od 5000 do 50 000 Kč/osoba) apod.

- Kritické dopady (koeficient 4)
  Zásadní nebo i nezvratné dopady, které se nemusí podařit překonat.
  Pro správce – fyzická újma (útoky na členy, zaměstnance společnosti, pracovní neschopnost), společenská újma (soudní proces, likvidace společnosti), finanční náklady nad 5 000 000 Kč nebo vznik nesplatitelného dluhu apod.
  Pro subjekty údajů – fyzická újma (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost), společenská újma (ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv), finanční újma (zneužití finančních prostředků, dodatečné náklady, škoda nad 50 000 Kč/osoba, neschopnost splácet dluh) apod.

- **Míra hrozby – pravděpodobnost události**
  Definuje se pomocí hodnoty vyjadřující četnost výskytu hrozeb.
  - Zanedbatelná pravděpodobnost (koeficient 1) – hrozby se nevyskytují nebo s víceletou periodou.
  - Nízká pravděpodobnost (koeficient 2) – frekvence výskytu hrozeb se pohybuje v ročním intervalu.
  - Významná pravděpodobnost (koeficient 3) – frekvence výskytu hrozeb se pohybuje v intervalu měsíců.
  - Kritická pravděpodobnost (koeficient 4) – frekvence výskytu hrozeb se pohybuje v intervalu dnů nebo kratších.

- **Míra zranitelnosti**
  Definuje se pomocí hodnoty vyjadřující využití zranitelnosti na základě přijatých opatření
  - Zanedbatelná zranitelnost (koeficient 1) – 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 o narušení integrity, dostupnosti a důvěrnosti osobních údajů (úspěšné pokusy nejsou známy); účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
  - Omezená zranitelnost (koeficient 2) – 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 o narušení integrity (úspěšné pokusy nejsou známy), dostupnosti a důvěrnosti osobních údajů; účinnost opatření je pravidelně kontrolována; opatření jsou pravidelně revidována.
  - Významná zranitelnost (koeficient 3) – 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.
  - Kritická zranitelnost (koeficient 4) – 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 rizika pro osobní údaje**

Na základě stanovených koeficientů pro hodnocení dopadů, hrozeb a zranitelností vypočteme míru rizika pro každou hrozbu. K tomu lze použít následující vzorec.

riziko pro osobní údaje = dopad + míra hrozby + míra zranitelnosti

Obecně tedy může riziko pro osobní údaje nabývat hodnot mezi 3-12. Výsledné hodnoty lze rozdělit do několika skupin dle jeho úrovně.

- **Riziko nízké** (hodnoty 3, 4, 5) – riziko je považováno za akceptovatelné.
- **Riziko střední** (hodnoty 6, 7) – riziko je vhodné snížit finančně méně nákladnými opatřeními, to znamená, že je možné riziko akceptovat, pokud by možná opatření byla nepřiměřeně nákladná.
- **Riziko vysoké** (hodnoty 8, 9, 10) – riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
- **Riziko kritické** (hodnoty 11, 12) – riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho eliminaci (považováno za vysoké riziko ve smyslu článku 36 odstavec 1).

Posouzení rizik lze provést 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, míra hrozby, míra zranitelnosti, riziko; přijatá opatření (uvede se číslo opatření ze seznamu zpracovaného správcem); rizika po přijetí opatření se sloupci dopady, míra hrozby, míra zranitelnosti, zbytkové riziko (viz následující strana).

úřad pro ochranu osobních údajů
the office for personal data protection

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 zranitelnosti	riziko
Data	Nedostatečné řízení přístupu k oú	Zneužití nebo neoprávněná modifikace oú	x		x	3	3	4	10
HW	Nedostatečná údržba ICT	Poškození nebo selhání technického vybavení		x		2	2	4	8
atd.									

Přijatá opatření	Riziko po přijetí opatření			
	dopady	míra hrozby	míra zranitelnosti	zbytkové riziko
1, 2*)	3	2	1	6
3, 4*)	2	2	1	5

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)*