Posouzení vlivu na ochranu osobních údajů (DPIA) Metodika

Jakub Míšek

Ústav práva a technologií PrF MU

Přehled prezentace

1. Právní úprava + smysl a účel DPIA
2. Kdy je DPIA potřeba
3. Postup při provádění posouzení

Právní úprava

- Čl. 35 GDPR
  - Popis povinností správce vzhledem k DPIA
  - Realizace principu odpovědnosti (čl. 24 GDPR)
- Interpretační vodítka WP29
  - 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, ze dne 4. dubna 2017, revidované k datu 4. října 2017

Smysl a účel DPIA

- Hlavní cíl – jistota, že správce řádně naplňuje povinnosti vyplývající z GDPR
  - Prevenční princip
- Rozdíl oproti běžnému managementu rizik:
  - Hodnotí se primárně riziko třetí osoby (subjekt údajů)
  - Ohrožena základní práva subjektu údajů
- Při hodnocení rizika je třeba brát v potaz zejména jeho původ, povahu, zvláštnost a závažnost
- Výsledek DPIA je třeba promítnout do samotného zpracování
  - Pokud je riziko příliš vysoké a správce ho nedokáže odstranit, zpracování nesmí proběhnout

Jaká zpracování mají být předmětem posouzení

- Čl. 35:
  - posouzení dopadů je třeba provádět v případech, kdy je pravděpodobné, že plánované zpracování osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob
    - Primárně právo na ochranu osobnosti soukromí a osobních údajů
    - Dále: právo na svobodu projevu, svobodu myšlení, svobodu pohybu, svobodu svědomí a náboženského vyznání
- „je pravděpodobné“
  - Není nezbytné před každým zpracováním
  - Je proto dobré dělat předběžné hodnocení dopadů
    - „zamyslet se“

Vysoké riziko zpracování - GDPR

- Rozsáhlé operace zpracování sloužící ke zpracování velkého množství osobních údajů
  - systematické a rozsáhlé profilování
  - automatizované rozhodování o právech a povinnostech subjektů údajů
  - rozsáhlé zpracování citlivých osobních údajů
  - rozsáhlé systematické monitorování veřejně přístupných prostor
- Masivní využití nových technologií
- Pro subjekty je obtížné u správce uplatnit svá práva
- Další zpracování představující vysoké riziko

Rizikové kategorie zpracování dle WP 29

1. Zpracování je prováděno za účelem hodnocení nebo bodování, profilování a předpovídání zejména na základě dat souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu.
   - vytváření behaviorálních nebo marketingových profilů na základě používání webových stránek nebo na základě znalosti předchozích koupí zboží
   - hodnocení žadatele o úvěr

Rizikové kategorie zpracování dle WP 29

2. Zpracování je prováděno za účelem automatizovaného rozhodování, které má právní nebo podobně závažný dopad, jinými slovy, kdy je přímo nebo nepřímo rozhodováno o právech a povinnostech subjektu údajů.

- automatizované rozhodování o přijetí ke studiu, o výplatách stipendií a podobně

Rizikové kategorie zpracování dle WP 29

3. Zpracování představuje systematické monitorování, pozorování nebo kontrolu subjektů údajů

- Včetně údajů shromážděných prostřednictvím sítí
- Rozsáhlé systematické monitorování veřejně přístupných prostorů.
- Problém - osobní údaje mohou být shromažďovány za okolností, za nichž nemusí subjekty údajů vědět, kým jsou jejich údaje shromažďovány a jak budou použity.

Rizikové kategorie zpracování dle WP 29

4. Zpracování citlivých osobních údajů, nebo údajů vysoce osobní povahy

- Zdravotnická dokumentace, nebo údaje výpisu z trestního rejstříku
- Citlivé údaje v obecném slova smyslu
  - Vypovídají o soukromém a osobním životě subjektu údajů, mají vazbu na jeho domácnost a soukromé činnosti
  - Údaje související s elektronickými komunikacemi (data i metadata, kterými jsou provozní a lokalizační údaje)
  - Finanční údaje, údaje, které by mohly vést ke krádeži identity
  - Pomocná otázka: řekl by je subjekt údajů sám veřejnosti?

Rizikové kategorie zpracování dle WP 29

5. Zpracování osobních údajů probíhá v rozsáhlém měřítku. Při hodnocení, zda je toto kritérium naplněno je třeba zvážit následující:

- Počet subjektů údajů vyjádřený číslem, nebo jako podíl příslušné populace
- Objem a rozsah jednotlivých osobních údajů, které jsou zpracovávány
- Doba zpracování údajů (doba jejich uchování správcem)
- Zeměpisný rozsah činnosti zpracování (zda je zpracování omezeno lokálně, nebo má regionální přesah)

Rizikové kategorie zpracování dle WP 29

6. Při zpracování osobních údajů dochází ke slučování datových zdrojů, nebo přiřazování dat z různých zdrojů k sobě.

- Pokud například data původně pocházejí od dvou nebo více různých správců údajů, nebo jen byla data původně sbírána za různými účely, a chystané zpracování tato data propojuje
  - oprávněné očekávání subjektů údajů, že s jejich údaji bude nakládáno předem daným způsobem, který se však v takovéto aplikaci mění.

Rizikové kategorie zpracování dle WP 29

7. Zpracování se týká zranitelných subjektů údajů.
   - mezi subjekty a správcem údajů může být větší nerovnováha (pro jednotlivce může být nemožné snadno vyslovit souhlas případně nesouhlas se zpracováním svých údajů, nebo vykonávat svá práva)
     - Děti
     - Zaměstnanci
     - Zranitelné skupiny obyvatelstva vyžadující zvláštní ochranu (osoby s duševní poruchou, žadatelé o azyl, starší osoby, pacienti)
     - Další osoby, u kterých je možné stanovit nerovnováhu ve vztahu mezi postavením subjektu a správce údajů.

Rizikové kategorie zpracování dle WP 29

8. Při zpracování osobních údajů dochází k použití nebo využívání nových technologických nebo organizačních řešení.

- Nová technologie – možná nepředvídaná a nečekaná rizika pro subjekty údajů
- Před jejím nasazením nutné provést posouzení vlivů zpracování, které umožní správci údajů rizikům porozumět a navrhnout účinná protiopatření na jejich limitaci.

Rizikové kategorie zpracování dle WP 29

9. Zpracování samotné brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy.

- Zpracování osobních údajů, na základě kterých banka rozhodne, zda svému zákazníkovi udělí úvěr, či nikoli.
- Důvodem pro zahrnutí tohoto kritéria je zajištění umožnění informovanosti subjektu údajů.

Poznámky WP29

- Pokud jsou splněny 2 kategorie, je třeba provést DPIA
- Pokud jsou zpracování typově podobná, stačí jedno provedení DPIA
- Potřeba pravidelného opakování DPIA, aby bylo zaručeno, že zpracování je stále prováděno v souladu se zákonem

Výjimky z povinnosti zpracovat DPIA

- Čl. 35 odst. 5 a 10
  - Seznam zpracování, u kterých není DPIA potřeba zveřejněný dozorovým úřadem
  - Zpracování je prováděno na základě zákonné povinnosti a posouzení bylo provedeno již zákonodárcem

WP 29 – případy, kdy není DPIA nutné

- Není pravděpodobné, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob
- Povaha, rozsah, kontext a účel zpracování jsou velmi podobné zpracování, pro které bylo posouzení vlivu na ochranu osobních údajů už provedeno
- Zpracování bylo zkontrolováno Úřadem pro ochranu osobních údajů před nabytím účinnosti GDPR, a podmínky provedení takového se nezměnily
- Zpracování je prováděno na základě právní povinnosti a hodnocení dopadů tohoto zpracování bylo již provedeno v průběhu legislativního procesu

Kdo má zpracovat posouzení

- Správce údajů
- Vnitřní nastavení v rámci organizace je na ní
  - Ne pověřenec pro ochranu osobních údajů
  - Na MU – garant zpracování osobních údajů
    - Ve spolupráci s dalšími garanty, nebo správcem informačního systému

Postup při provádění posouzení

Krok 1 – Vyhodnocení cílů a relevance hodnocení

- Jak vyplývá z dalších povinností správce, při návrhu zpracování je třeba sledovat následující cíle:
  - **Minimalizace dat** – měly by být zpracovávány jen ty údaje, které jsou relevantní k danému účelu zpracování, a to jen po dobu, která je vzhledem k tomto účelu nutná.
  - **Dostupnost** – tento cíl směřuje k zajištění dostupnosti příslušných údajů a je zpracovávajících systémů pro správce/zpracovatele (v souladu s daným účelem – čl. 32 (1) a 5 (1) GDPR) a subjekt údajů (za účelem výkonu práv na přístup či přenositelnost – čl. 13, 15 a 20 GDPR).
  - **Integrita** – směřující k zajištění dat vůči neautorizované modifikaci nebo výmazu. Požadavek vyplývá z požadavků na zpracování dat (čl. 5 (1) (f) GDPR) a jeho bezpečnosti (čl. 32 (1) (b) GDPR).

Krok 1 – Vyhodnocení cílů a relevance hodnocení

- **Důvěrnost** – znamená ochranu před neautorizovanému nebo protiprávnímu zpracování. Požadavek na její zajištění vyplývá mimo jiné z čl. 5 (1) (f), 32 (1) (b), či 28 (3) (b) GDPR.
- **Nespojitelnost** – osobní údaje by měly být zpracovávány za účely, ke kterým byly shromážděny, nemělo by tak docházet ke spojování údajů shromážděných k různým účelům. Tento požadavek vyplývá mimo jiné z čl. 6, 5 (1) (b) a 7 (4) GDPR.
- **Transparentnost** – princip transparentnosti je zakotven v čl. 5 (1) (a) GDPR a jeho provedení se vyskytuje na několika místech nařízení. Souvisí především s informační povinností správce vůči subjektu údajů a dozorovému orgánu.
- **Ovlivnitelnost** – vychází z práva subjektu údajů ovlivňovat nakládání s nimi, tento požadavek je realizován především právy subjektu na opravu, blokování, výmaz, transfer a námitku (čl. 16 – 17 GDPR).

Krok 1 – Vyhodnocení cílů a relevance hodnocení

Kritéria determinující míru možného zásahu do práv subjektů údajů

- Míra monitorování subjektu údajů
- Klasifikace údajů shromažďovaných o subjektu
- Míra zranitelnosti subjektu údajů
- Dostupnost osobních údajů
- Rozsah zpracování osobních údajů
- Zasažené území
- Uplatnění práv subjektu údajů
- Přístupnost osobních údajů
- Soustavnost zpracování osobních údajů
- Transfer osobních údajů
- Působnost správce/zpracovatele
- Uzemní rozložení správce/zpracovatele
- Složitost sytému zpracování
- Vazby na jiné subjekty
- Inovativnost zpracování

Krok 2 – Zahájení

- Nashromáždění podkladů pro hodnocení
  - relevantní legislativa
  - interní normy
  - organizační předpisy
  - metodiky a manuály
  - organizační struktura
  - dokumentace informačního systému
  - grafy a diagramy popisující informační procesy
  - popis životního cyklu osobních údajů nebo obecně informací v systému
  - dokumentace bezpečnostních prvků infrastruktur

Krok 2 – Zahájení

- Nashromáždění podkladů pro hodnocení
  - Konzultace s relevantními osobami
    - Ideálně v průběhu celého procesu posouzení
    - Interní i externí
    - Pověřenec pro ochranu osobních údajů
    - Management
    - Dodavatelé a smluvní dodavatelé osobních údajů
    - Právní oddělení/odbor
    - Dohledové pracoviště CSIRT
    - Uživatelé systému
    - Výzkumníci

Krok 3 - Identifikace, charakterizace a popis hodnoceného informačního systému

- Zmapování informačního systému
- Popis informačních toků
  - Jak jsou data předávána a jejich životní cyklus
- Funkční dekompozice
  - Identifikace jednotlivých funkcí, které IS zastává
  - Identifikace účelu zpracování
  - Příklad MU:
    - Provozní funkce (evidence majetku, zaměstnanců…)
    - Funkce klíčových aktivit (realizace výuky a výzkumu)
    - Podpůrné funkce (podpora realizace dalších aktivit)

Krok 3 - Identifikace, charakterizace a popis hodnoceného informačního systému

- Komponentová dekompozice
  - Popis jednotlivých komponent příslušných systémů a modelování jejich skladebnosti
    - Konkrétní zařízení (prvek síťové infrastruktury, počítač…)
    - Dílčí části zařízení (moduly informačního systému)
    - Subsystémy (komunikační systém zajišťující komunikaci mezi zařízeními pro sběr dat a datovou centrálou)
  - Příklady komponent:
    - Hardware: počítače, pevná a přenosná úložiště, senzory, inteligentní zařízení, pracovní stanice, servery apod.,
    - Software: operační systémy, databázové systémy, aplikace a informační systémy, moduly systémů apod.,
    - Sítě: síťové a napěťové vedení, routery, switche, access pointy apod.,
    - Lidé: uživatelé, administrátoři, správci apod.,
    - Dokumenty: papírové dokumenty, archiv, složky, smluvní dokumenty, papírová evidence, apod.
  - Význam: identifikace komponent s jejichž užitím může souviset výskyt nebo možnost výskytu rizika

Krok 4 - Identifikace relevantních rizik

- Nezbytné identifikovat možná rizika, která se mohou vyskytnou při zpracování údajů
  - Zpravidla vázána na komponenty systému
- Základní princip posouzení – proces ve formě řízení rizik
- Riziko vůči subjektu údajů bude zpravidla souviset s rizikem vzniku odpovědnosti na straně správce údajů

Krok 4 - Identifikace relevantních rizik

- Příklady rizik pro subjekt údajů:
  - Nevhodné sdílení osobních údajů,
  - využití údajů pro účely odlišné od účelů pro které byly získány,
  - neoprávněný zásah do soukromí,
  - rozhodování o právech subjektu na základě neoprávněného zpracování údajů,
  - ohrožení soukromí díky neoprávněnému slučování údajů z různých zdrojů a profilování,
  - sběr identifikátorů znemožňujících anonymní využití služby,
  - zpětná identifikace pseudonymizovaných údajů,
  - nedostatečně efektivní anonymizace dat,
  - neúčelné zpracování osobních údajů,
  - zbytečné uchovávání nepotřebných údajů

Krok 4 - Identifikace relevantních rizik

- Příklady rizik pro správce údajů:
  - sankce, pokuty
  - poškození reputace
  - nákladné změny v chybném mechanismu zpracování údajů
  - přílišný dohled může odradit zájemce o studium nebo spolupráci
  - zbytečné plýtvání výpočetními zdroji na zpracování nepotřebných údajů,
  - možnost vzniku odpovědnosti za škodu

Krok 5 – Vyhodnocení rizik

- Hodnocení z hlediska významnosti dopadu a z hlediska pravděpodobnosti výskytu události
- 4 stupně hodnotící škály (zanedbatelná, omezena, významná, maximální)
- Hodnocené oblasti:
  - Významnost dopadu
    - Riziko možnosti identifikace subjektu údajů
    - Riziko možnosti zásahu do práv subjektu údajů
  - Pravděpodobnost výskytu
    - Zranitelnost komponent
    - Schopnost zdrojů hrozby využít zranitelnosti

Krok 5 – Vyhodnocení rizik

- Rizika s významným dopadem a pravděpodobností výskytu
  - musí být zcela jednoznačně vyřešena nebo limitována přijetím vhodných technických a organizačních opatření k omezení jejich dopadů a pravděpodobností výskytu. Zvolená opatření by měla mít charakter jak preventivní, tak i ochranný (schopnost reakce) a nápravný (snížení dopadů již vzniklé hrozby)
- Rizika s významnými dopady ale malou pravděpodobností výskytu
  - musí být vyřešena nebo limitována opatřeními, které omezí jejich potenciální dopady, nebo zcela redukují pravděpodobnost výskytu. Pozornost by měla být především věnována implementace preventivních opatření.

Krok 5 – Vyhodnocení rizik

- Rizika s malým dopadem ale vysokou pravděpodobností výskytu
  - musí být omezena prostřednictvím opatření směřujících ke snížení pravděpodobnosti výskytu hrozby. Důraz by měl být kladen na nápravná opatření při výskytu hrozby
- Rizika s malým dopadem a malou pravděpodobností výskytu
  - nemusí být nutně řešena, nebo mohou být pokryta opatřeními směřujícími vůči jiným rizikům

Krok 6 - Vyhodnocení bezpečnostních opatření

- Možnosti vyřešení rizika:
  - Modifikace rizika
    - riziko je vyloučeno nebo omezeno prostřednictvím volby a implementace vhodných organizačních a technických opatření
  - Přijetí rizika
    - riziko je vyhodnoceno jako nízké a implementace dodatečných opatření se nejeví jako účelná nebo proporciální (nutné odůvodnění a dokumentace)
  - Vyloučení rizika
    - absolutní vyloučení rizika tím, že zpracování vůbec nezačne, nebo bude ukončeno
  - Sdílení rizika
    - v rámci organizace nebo i mimo ni existují subjekty které jsou schopny riziko převzít a disponují nástroji na jeho vyloučení (například lze provozem systému pověřit jinou organizační jednotku)

Krok 7 - Dokumentace a návrh závěrečné zprávy

- Žádný předepsaná forma
- Obsahuje informace relevantní pro posouzení vhodnosti a účelnosti přijatých organizačních a technických opatření
- Popisuje probíhající zpracování, realizované kroky posouzení, identifikovaná rizika a vyrovnání se s nimi

Krok 8 – Revize, údržba

- Nastavení mechanismů údržby nastaveného systému bezpečnostních opatření
  - Př. Při provozu dojde k objevení zranitelnosti, je třeba ji řešit
- Mechanismus pravidelné kontroly a revize nastaveného systému ochrany osobních údajů
- V dokumentaci by mělo být uvedeno, jak často, případně za jakých podmínek, revize bude probíhat

= Nové zpracování DPIA

- Zaměřené na změny, které proběhly od posledního vypracování
  - Změny například v podobě nových technologií, nově objevené hrozby a zranitelnosti

Děkuji za pozornost.

@jkb_misek