EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

SPISOVÁ A ARCHIVNÍ SLUŽBA

Celkové zhodnocení zpracování a ochrany osobních údajů

Metodický list

Autor: Ing. Petr Hlaváč, Metodik: Ing. Vladimír Šulc, Ph.D.

Recenzent: Ing. Vojtěch Hvězda

Rok vydání: 2023)

Osnova

Cíle

- Žák popíše celý postup pro vyhotovení analýzy zpracování a ochrany osobních údajů
- Žák osvětlí, jaký mají riziková zpracování vliv na bezpečnost a ochranu osobních údajů
- Žák vysvětlí, kdy a proč by provedl analýzu v organizaci znovu

Dovednosti

- Žák provede celkové zhodnocení práce na analýze zpracování osobních údajů
- Žák navrhne opatření, jak snížit riziková zpracování, a také, jak zvýšit ochranu osobních údajů
- Žák za pomoci získaných znalostí a dovedností zdůvodní veškeré provedené kroky

Pracovní prostředí

Úlohu lze realizovat v prostředí JCEKB

Pro práci budeme potřebovat následující:

- Připojení k internetu a webový prohlížeč (Google Chrome, Microsoft Edge)
- Přístup do aplikace GDA (alespoň pro vyučujícího)

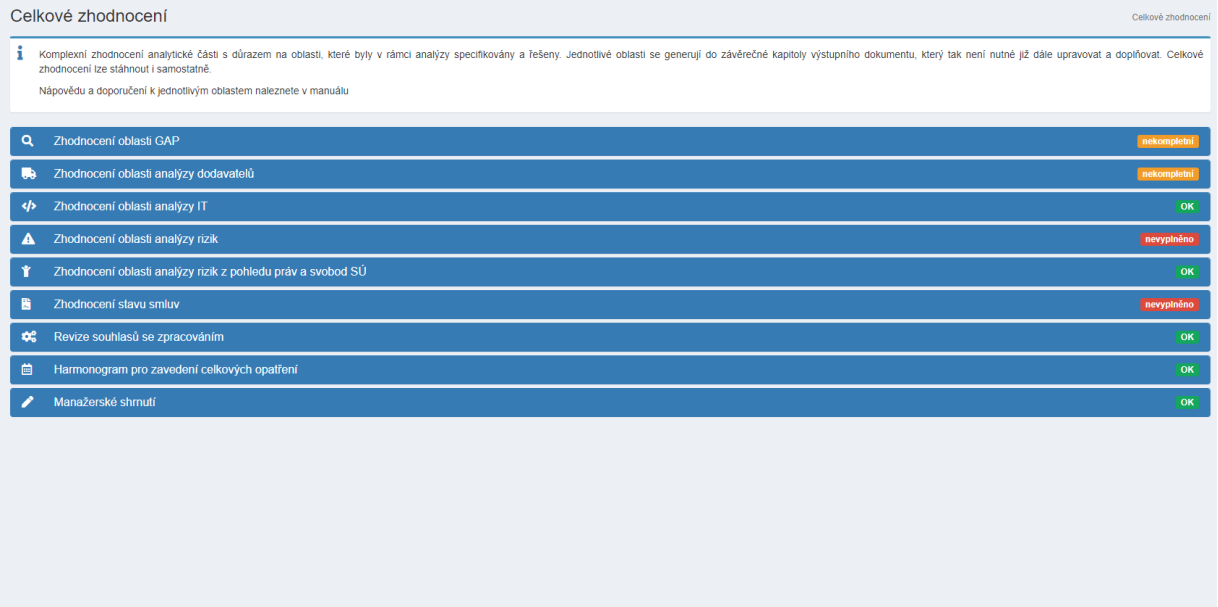
Průběh výuky

1 Příprava

Prvních 20–30 minut diskuse a výklad na téma správného postupu při analýze zpracování a ochrany osobních údajů. Vysvětlení nejdůležitějších pojmů. Určení modelové organizace, která bude hodnocena včetně jejich parametrů. Přihlášení do aplikace GDA.

2 Celkové zhodnocení

Komplexní zhodnocení analytické části s důrazem na oblasti, které byly v rámci analýzy specifikovány a řešeny. Jednotlivé oblasti se generují do závěrečné kapitoly výstupního dokumentu, který tak není nutné již dále upravovat a doplňovat. Celkové zhodnocení lze stáhnout i samostatně.



Zhodnocení oblasti GAP

V této části dochází k rozboru nejzávažnějších nesouladů organizace vůči nařízení GDPR. GAP analýza přesně kopíruje znění samotného nařízení GDPR. Organizace získá jasný přehled o tom, ve kterých oblastech nařízení plní, a ve kterých již nikoliv. Velmi závažné neshody vůči nařízení budou podrobněji rozebrány v této části. Na ně navazují doporučená opatření, která by měla organizace k odstranění či minimalizaci rozporů přijmout. Ve většině případů organizace nedokáže naplnit veškerá ustanovení, která GAP analýza zahrnuje. Nicméně vždy musí mít zavedený buď formální proces či funkční softwarový nástroj, díky kterému dokáže plnit práva subjektu údajů a povinnosti plynoucí nařízení z GDPR.

Navrhovaný postup:

- Vygenerujte si dokument "***GAP***" ve formátu .docx v sekci *Dokumenty*. 
- Na základě informací v kapitole "***Zvláště významné neshody***" vyberte oblasti, u kterých identifikujete největší možné riziko pro SÚ a analyzovanou organizaci.
- K těmto neshodám je vhodné vytvořit plány opatření, kterými budou neshody odstraněny, případně minimalizovány.

Zhodnocení oblasti analýzy dodavatelů

Organizace musí získat vyjádření dodavatelů informačních systémů, ve kterých se zpracovávají osobní údaje, jež jasně specifikuje zabezpečení daného systému a jeho připravenost na GDPR. Jedná se zejména o systémy, ve kterých se zpracovává mzdová a personální agenda či CRM systémy a databáze klientů. Pokud organizace najde v této oblasti nedostatky (např. špatné zabezpečení systému, zastaralé verze bez aktualizace, nulovou přípravu dodavatele na GDPR), musí připravit systém opatření, jenž bude dané nedostatky řešit. Ve většině případů se nabízí přechod na novější (bezpečnější) verzi systému nebo jeho kompletní výměna. Organizace by měla vždy dbát na to, aby veškeré její systémy (a zejména bezpečnostní) byly navzájem kompatibilní.

Navrhovaný postup:

- Vygenerujte si dokument "***Analýza SW***" ve formátu .docx v sekci *Dokumenty*. 
- Na základě informací k jednotlivým systémům, které jsou obsaženy ve staženém dokumentu, najděte jejich největší slabiny a navrhněte možná opatření.

Zhodnocení oblasti analýzy IT

Špatný stav IT organizace představuje jasné ohrožení zabezpečení osobních údajů. V této části dochází k popisu a rozboru největších nedostatků v oblasti IT, které musí organizace jednoznačně řešit. Zajistí tím zlepšení úrovně informační bezpečnosti i ochrany osobních údajů. Mezi tyto nedostatky spadá např. zastaralý hardware (stáří více než 5 let) nebo chybějící zabezpečení koncových stanic (špatný identity management, nezabezpečené porty...).

Navrhovaný postup:

- Vygenerujte si dokument "***Analýza IT***" ve formátu .docx v sekci *Dokumenty*. 
- Na základě informací v oblastech informační infrastruktury, které jsou obsaženy ve staženém dokumentu, najděte největší slabiny a navrhněte možná opatření, jež tyto slabiny eliminují.

Zhodnocení oblasti analýzy rizik

Následující část jmenuje a popisuje nejvíce riziková zpracování osobních údajů v organizaci. Veškerá riziková zpracování musí organizace chápat v kontextu celé své praxe. Nejvíce se ovšem musí organizace zaměřit na rizika, která přímo ohrožují práva a svobody garantované subjektům údajů (lidem) dle nařízení GDPR a Listiny základních práv EU. Záměrné či nahodilé zkreslení, únik nebo přímo zneužití osobních údajů mohou výrazně ohrozit práva jednotlivce.

Organizace tak musí zavést systém opatření, který minimalizuje rizika pro subjekt údajů, ale i pro samotnou organizaci (hrozba úniku) a zabezpečení osobních údajů. Při revizi analýzy GDPR by již organizace neměla mít žádná riziková zpracování.

Navrhovaný postup:

- Vygenerujte si dokumenty "**Analýza rizikových zpracování osobních údajů**", "**Analýza rizikových zpracování osobních údajů z pohledu práv a svobod subjektu údajů**" a "***Inventarizace a klasifikace osobních údajů***" v sekci *Dokumenty*.

- Na základě rizikových zpracování definujte možné postupy, kterými můžete rizika minimalizovat či úplně odstranit.

Zhodnocení oblasti stavu smluv

- Organizace si projde veškeré smlouvy, které předkládá třetím stranám. Jedná se zejména o pracovní smlouvy, obchodní smlouvy, zpracovatelské, smlouvy s partnery atd.
- Organizace by měla ve smlouvách vždy specifikovat, jakým způsobem bude nakládáno se svěřenými osobními údaji a o jaké konkrétní osobní údaje se jedná. Například v rámci pracovních smluv by organizace měla specifikovat, jaké osobní údaje od zaměstnance potřebuje a kde se tyto údaje mohou objevit (např. na webu, na prezentačních materiálech, v časopise apod.).
- Organizace by měla vždy protistranu o těchto skutečnostech jasně informovat. Ovšem měla by se vyhnout podepisování specifických "souhlasů se zpracováním osobních údajů", jakožto samostatného dokumentu, neboť funkci takových souhlasů více upřesňuje samotné nařízení GDPR, které je činí v praxi pro většinu organizací méně využitelné než doposud.
- Organizace také prověří smlouvy se subjekty, jež za ni nějakým způsobem zpracovávají (spravují) osobní údaje. V tomto směru by organizace měla disponovat jasným vyjádřením, jaké osobní údaje protistrana zpracovává a jakým způsobem jsou zabezpečeny.
- V neposlední řadě se organizace v tomto bodě zaměří i na své vnitřní dokumenty týkající zpracování, nakládání a zabezpečení osobních údajů i zajištění kybernetické bezpečnosti organizace, protože její úroveň má obrovský vliv na celkové zabezpečení osobních údajů.
- Organizace by tak měla disponovat směrnicemi kybernetické bezpečnosti a směrnicemi pro zpracování a zabezpečení osobních údajů. Nicméně samotná směrnice Zabezpečení osobních údajů problém neřeší. Nastaví jasná pravidla pro zaměstnance, třetí strany, partnery a další osoby, které jsou relevantní pro danou činnost. Dá směr, jak zpracovávat v organizaci osobní údaje. Pro celkové zlepšení zabezpečení osobních údajů musí být tyto směrnice uvedeny v praxi.

Pokud organizace zjistí v jakémkoliv z výše zmíněných bodů nedostatek, je třeba jej co nejdříve odstranit.

Revize souhlasů se zpracováním

Nařízení GDPR významně mění podobu a funkci souhlasu se zpracováním osobních údajů. Ve většině organizací bude muset dojít ke změně znění souhlasu se zpracováním osobních údajů, respektive k

jejich aktualizaci. Souhlasy pořízené podle staré legislativy **nejsou dle současných právních předpisů platné**. Je nutné vyhnout se odkazům na starou legislativu. V případě nutnosti souhlasu je třeba mít souhlas v podobě, která nese jasné parametry nařízení, tedy: jednoznačný, účelový, přesně vymezený...

Harmonogram pro zavedení opatření

Na základě zjištěných nedostatků z jednotlivých kapitol a na nich navazujících doporučení si organizace sestavuje časový harmonogram realizace opatření, která jí pomohou zavést povinnosti vyplývající z nařízení GDPR. Organizace vždy zavádí opatření dle logické posloupnosti od jednodušších po složitější. Zavedená opatření musí vést ke zlepšení současného stavu. Celá organizace se s nimi musí ztotožnit a zejména podle nich jednat.

Ilustrační příklad harmonogramu:

Priorita	Název doporučení	Popis doporučení	Datum realizace
Technická opatření			
3	PDIL	Pořízení nástroje pro mapování a vyhledávání osobních údajů v databázích a dokumentech	11.4.2024
Procesní a organizační opatření			
1	DPO	Zavedení Pověřence pro ochranu osobních údajů	15.2.2024
2	Revize a aktualizace smluv	Kontrola veškerých z naší strany překládaných smluv a jejich případná aktualizace	30.3.2024

Manažerské shrnutí

V této části autor analýzy shrne veškerá významná zjištění, zejména pak nedostatky organizace v plnění nařízení GDPR. Zároveň je vhodné, aby se autor vyjádřil, za jak dlouho si myslí, že je organizace schopna nařízení zavést do své praxe. V této části má také autor možnost vyjádřit se k dalším skutečnostem, které nezmínil v jiných pasážích. Autor analýzy by měl mít na paměti, že právě manažerské zhodnocení a harmonogram opatření patří mezi nejdůležitější části samotné analýzy.

Shrnutí a závěr

Žáci během dvou vyučovacích hodin provedou celkové zhodnocení práce na analýze zpracování a ochrany osobních údajů navrhnou alespoň tři opatření pro zvýšení ochrany osobních údajů. Vyučující zhodnotí navržená opatření a celkový postup žáků v rámci analýzy. Společně doladí případné nedostatky a výzvy. Tato část bude rovněž vyučována za pomoci aplikace GDA.

Seznam použitých zdrojů

1. https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679
2. https://www.zakonyprolidi.cz/cs/2019-110
3. https://demo.app.gordiccybersec.cz/analysis/Zwx0w/divisions-and-roles-definition/?do=showManual