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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

SPISOVÁ A ARCHIVNÍ SLUŽBA

Inventarizace a analýza osobních údajů

Metodický list

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

Recenzent: Ing. Vojtěch Hvězda

Rok vydání: 2023

Obsah

Cíle

- Žák popíše různé atributy (pojmy), které se váží k osobním údajům
- Žák osvětlí, jaký vliv mají různé hodnoty na zpracování a ochranu osobních údajů
- Žák vysvětlí, proč je nutné provádět pravidelnou inventarizaci a analýzu rizikových zpracování osobních údajů

Dovednosti

- Žák provede inventarizaci a analýzu rizikových zpracování osobních údajů
- Žák dokáže samostatně přiřadit veškeré hodnoty a atributy k jednotlivým zpracováním
- Žák za pomocí získaných znalostí zdůvodní hodnocení provedená v těchto částech

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)

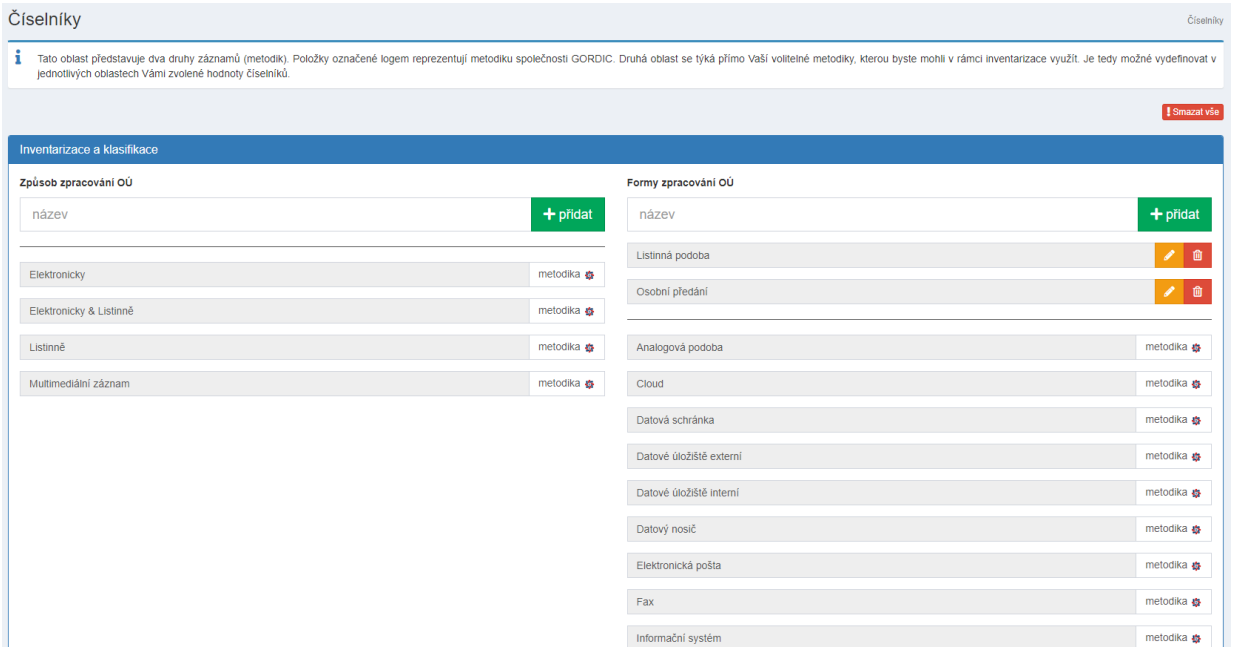
Průběh výuky

1 Příprava

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

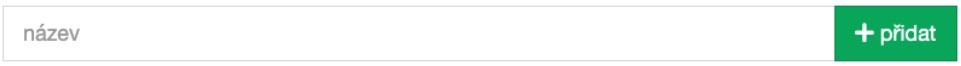
2 Číselníky

Tato oblast představuje dva druhy záznamů (metodik). Položky označené logem reprezentují metodiku společnosti Gordicu vycházející z platné legislativy. Druhá oblast se týká přímo volitelné metodiky, kterou bychom mohli v rámci inventarizace využít. Je tedy možné vydefinovat v jednotlivých oblastech zvolené hodnoty číselníků**.** Ovšem tvůrce doporučuje se držet předem definované metodiky.



Vytvoření vlastní položky číselníku:

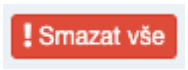
- U příslušného číselníku vyplňte název a stiskněte funkci + **přidat**



U vlastních položek číselníku pak lze provádět následující operace:

- **Odstranění** stisknutím červeného symbolu koše u příslušného záznamu
- **Editace** stisknutím oranžového symbolu tužky u příslušného záznamu

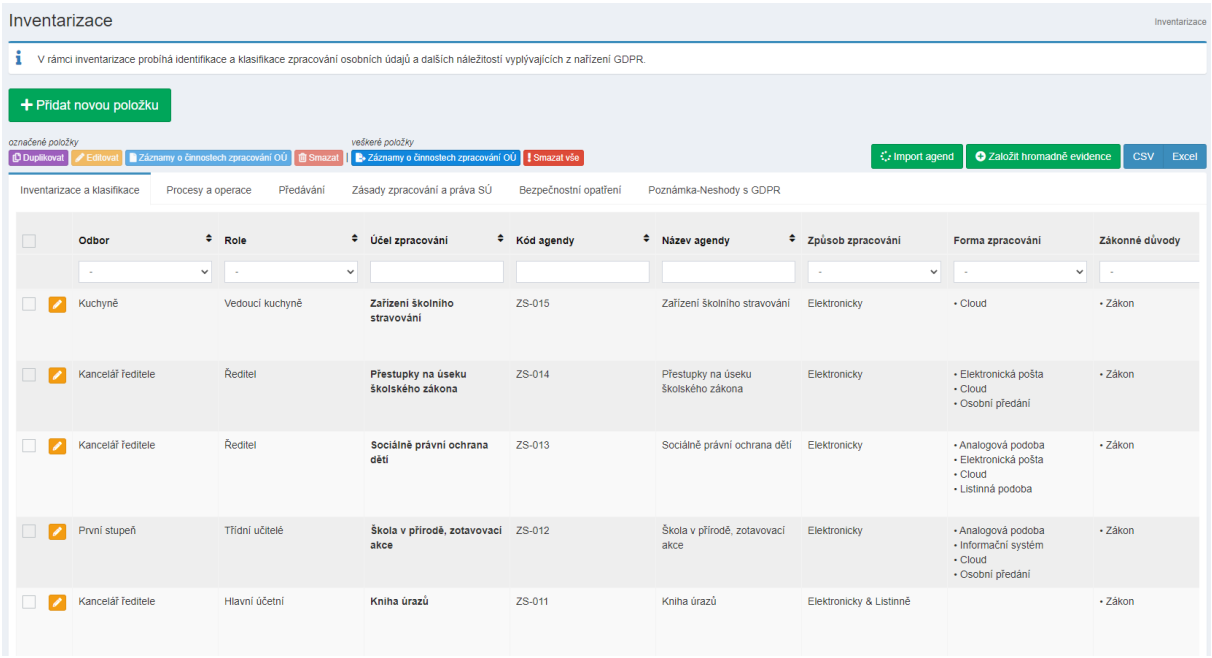
- **Hromadné odstranění** všech vlastních záznamů stisknutím funkce **!smazat vše**



U hromadného odstranění budete vyzvání k zadání hesla Vašeho účtu, po jehož ověření bude hromadné odstranění dokončeno.

3 Inventarizace

V rámci inventarizace probíhá identifikace a klasifikace zpracování osobních údajů a dalších náležitostí vyplývajících z nařízení GDPR. Jedná se o jednu z nejdůležitějších a nejnáročnějších částí v rámci celého procesu zpracování osobních údajů. Nutné je projít a doplnit veškeré údaje k inventarizačním zpracování.



Položky inventarizace jsou zobrazené nebo skryté v závislosti na vyplněném dotazníku v sekci *Dotazník.* Tím je zajištěna inventarizace na míru Vaší společnosti a eliminace času potřebného k opakovanému vyplňování irelevantních položek.

Agendy pro inventarizaci lze přidávat dvěma způsoby:

1) Postupně

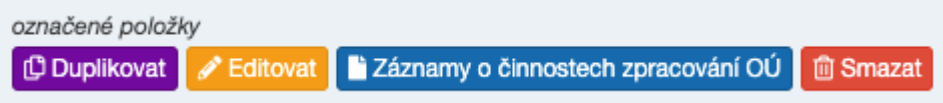
- Stiskněte funkci **+ Přidat novou položku**
- Vyplňte příslušné informace v záložkách *Inventarizace a klasifikace, Procesy a operace, Předávání, Zásady zpracování a správa SÚ, Bezpečnostní opatření* a *Dokončení*
- Stiskněte zelenou funkci **Dokončit**

2) Hromadně

- Stiskněte zelenou funkci **Import agend**

Importují se všechny agendy ze sekce *Analýza agend,* které doposud nebyly importovány.

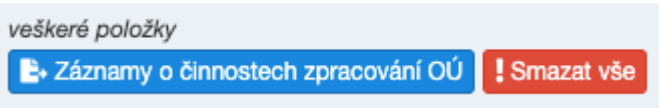
Se záznamy v Inventarizaci lze provádět hromadné operace:



- Vyberte záznamy, u kterých chcete provést změnu
- Stisknutím funkce **Duplikovat** vytvoříte kopie vybraných záznamů *Inventarizace*
- Stisknutím funkce **Editovat** provedete hromadnou úpravu vybraných záznamů *Inventarizace*

pozn. editaci lze provádět i na úrovni záznamů stisknutím oranžové funkce se symbolem tužky

- Stisknutím funkce **Záznamy o činnostech zpracování OÚ** se na Vaše zařízení uloží soubor (formát .zip) s komprimovanými soubory (formát .docx) - Záznamy o činnostech zpracování OÚ - vybraných záznamů *Inventarizace*
- Stisknutím funkce **Smazat** odstraníte vybrané záznamy *Inventarizace*



- Stisknutím funkce **Záznamy o činnostech zpracování OÚ** se na Vaše zařízení uloží soubor (formát .zip) s komprimovanými soubory (formát .docx) - Záznamy o činnostech zpracování OÚ - všech záznamů *Inventarizace*
- Stisknutím funkce **"!Smazat vše"** odstraníte všechny záznamy *Inventarizace* (označené i neoznačené)

U hromadného odstranění budete vyzváni k zadání hesla Vašeho účtu, po jehož ověření bude hromadné odstranění dokončeno.

Celou Inventarizaci lze exportovat:

- do souboru .csv stisknutím funkce **CSV** – data jsou jednom pracovním listu
- do souboru .xlsx stisknutím funkce **Excel** – data jsou rozdělena do více pracovních listů

Další dostupné funkce:

- Reload dat agendy 
- Načtení všech dostupných dat 

Geografická lokalizace

Geografická lokalizace OÚ definována v záložce **"Číselníky"** - jedná se o to, kde jsou data uložena z pohledu geografické polohy - V Evropské unii, Mimo EU.

Procesy životního cyklu OÚ

Procesy životního cyklu OÚ definovány v záložce **"Číselníky"** - jedná se o procesy plynoucí z know-how. Pořizování osobních údajů, Ukládání osobních údajů v úložištích, Přenosy při zpracování osobních údajů, Zpřístupnění při zpracování osobních údajů, Změna při zpracování osobních údajů, Přístup přes rozhraní k osobním údajům, Sdílený přístup k osobním údajům, Zálohování osobních údajů, Archivace osobních údajů a Likvidace osobních údajů.

Operace zpracování

Operace zpracování OÚ definovány v záložce **"Číselníky"** - jedná se o operace zpracování OÚ plynoucí z GDPR – shromáždění, zaznamenání, uspořádání, strukturování, uložení, pozměnění, vyhledání, nahlédnutí, použití, přenos, šíření, seřazení, omezení, výmaz a zničení.

Správce / Zpracovatel

Správce/zpracovatel OÚ definován v záložce **"Číselníky"** - pro dané zpracování určuje, zda jej provádí "Správce" nebo "Zpracovatel".

Monitoring zpracování

Je prováděn monitoring daného zpracování – ANO/NE.

Správce řeší porušení zabezpečení osobních údajů požadovaným způsobem

Je při porušení zabezpečení osobních údajů toto porušení řešeno jejich správcem požadovaným způsobem? Nařízení GDPR článek 33 - ANO/NE.

Zpracovatel řeší porušení zabezpečení osobních údajů požadovaným způsobem

Je při porušení zabezpečení osobních údajů toto porušení řešeno jejich zpracovatelem požadovaným způsobem? Odkaz na METODIKU článek 34 - ANO/NE.

Způsoby aktualizace OÚ

Způsoby aktualizace OÚ definované v záložce **"Číselníky"** - jedná se o způsob aktualizace OÚ - jakým způsobem jsou osobní údaje udržovány v aktualizovaném stavu.

Software

Software definován v záložce **"Číselníky"** - jedná se o informační systémy, ve kterých jsou OÚ zpracovávány.

Profilování

Automatické vyhodnocování na základě sběru OÚ, profilování. Jedná se například o situaci, kdy na základě předchozích nákupů v supermarketu při držení věrnostní karty analyzuji provedené nákupy a poskytuji slevy zákazníkovi na jím preferované výrobky – ANO/NE

Nad účel

Jsou zpracovávány OÚ nad účel legislativních či jiných účelů zpracování – ANO/NE

Předávání údajů v rámci organizace

Předávají se osobní údaje zpracovávané v daném zpracování k dalšímu zpracování v rámci organizace? - ANO/NE.

Zpřístupnění údajů třetím stranám

Jsou osobní údaje zpracovávané v daném zpracování zpřístupněny/předávány třetím stranám (externí subjekty, organizace, orgány atd.)? - ANO/NE.

Zásady předávání

Zásady předávání definovány v záložce **"Číselníky"** - jedná se podnět pro předávání OÚ do třetích zemí nebo v rámci korporátních organizací. - Předání založené na rozhodnutí o odpovídající ochraně, Předávání založené na vhodných zárukách, Závazná podniková pravidla předávání, Předání či zveřejnění údajů nepovolená právem Unie, Výjimky pro specifické situace, Mezinárodní spolupráce v zájmu ochrany osobních údajů.

Zásady zpracování OÚ

Zásady zpracování OÚ definovány v záložce **"Číselníky"** - jedná se o zásady zpracování OÚ plynoucí z GDPR. Dané zásady mohou být následující – Jsou definovány a srozumitelně popsány, jsou zákonné (nesmí se jednat o zpracování v rozporu s právními předpisy ČR nebo EU), data jsou zpracovávána způsobem, který je slučitelný s definovanými účely, zpracování pro účely statistické,

archivace ve veřejném zájmu a vědeckého či historického výzkumu se nepovažují za neslučitelné s původními účely.

Doba aktivního užití dokumentu

Doba aktivního užití dokumentu definována v záložce **"Číselníky"** - jedná se o položku závislou na účelu zpracování a možné odpovědi jsou následující – Novela zákona, Vypršení smlouvy, Zrušení souhlasu (Odvolání) a další.

Doba archivace neaktivního dokumentu (skartační znaky)

Definování skartačních znaků dle spisového a skartačního plánu.

Způsob skartace

Způsob skartace definován v záložce **"Číselníky"** - jedná se o způsob, jakým byl dokument skartován – Fyzicky, elektronicky a jinými způsoby.

Práva přístupu subjektů údajů k svým OÚ

Má subjekt údajů přístup ke svým osobním údajům zpracovávaných Vaší organizací? - ANO/NE.

Právo na opravu

Má subjekt údajů právo na opravu svých osobních údajů zpracovávaných Vaší organizací? - ANO/NE.

Právo na výmaz („právo být zapomenut“)

Má subjekt údajů právo na výmaz svých osobních údajů zpracovávaných Vaší organizací? - ANO/NE.

Právo na omezení zpracování

Má subjekt údajů právo na omezení zpracování svých osobních údajů zpracovávaných Vaší organizací? Tedy v případě nutnosti pozastavit všechny činnosti zpracování daného osobního údaje? - ANO/NE.

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Má správce povinnost oznámit subjektu údajů jakoukoliv změnu, omezení či výmaz OÚ – ANO/NE.

Právo na přenositelnost údajů

Má subjekt údajů právo na přenositelnost svých osobních údajů zpracovávaných Vaší organizací? - ANO/NE.

Právo vznést námitku

Má subjekt údajů právo vznést námitku na Vaši organizaci? - ANO/NE.

Přístup k údajům

Role v organizaci definována v záložce **"Definice organizace"**.

Pseudonymizace

Je v rámci daného zpracování zavedena pseudonymizace – ANO/NE.

Šifrování

Jsou dané osobní údaje v rámci daného zpracování šifrována – ANO/NE.

Zavedená bezpečnostní opatření

Bezpečnostní opatření definována v záložce **"Číselníky"** - otázka zní, zda jsou v daném zpracování zavedena jakákoliv opatření plynoucí z předchozí analýzy rizik, může jít o opatření – Technické, Organizační nebo Procesní.

Popis opatření

Slovní popis k zavedeným bezpečnostním opatřením.

Posouzení vlivu na ochranu osobních údajů

Předpokládáte u daného zpracování OÚ posouzení vlivu na ochranu osobních údajů? Jedná se především o maximálně riziková zpracování, která se ve většině případů vyskytovat nebudou. - ANO/NE.

Předchozí konzultace s dozorovým úřadem

Měli jste v rámci daného zpracování předchozí konzultaci s dozorovým orgánem ÚOOÚ? - ANO/NE.

Kodex

Podepsal správce údajů kodex chovaní vůči subjektu údajů – ANO/NE.

Monitoring plnění kodexu

Probíhá monitoring kodexu chovaní správcem údajů vůči subjektu údajů – ANO/NE.

Osvědčení

Doplňte název osvědčení, které vlastníte v souvislosti s GDPR.

4 Analýza rizik

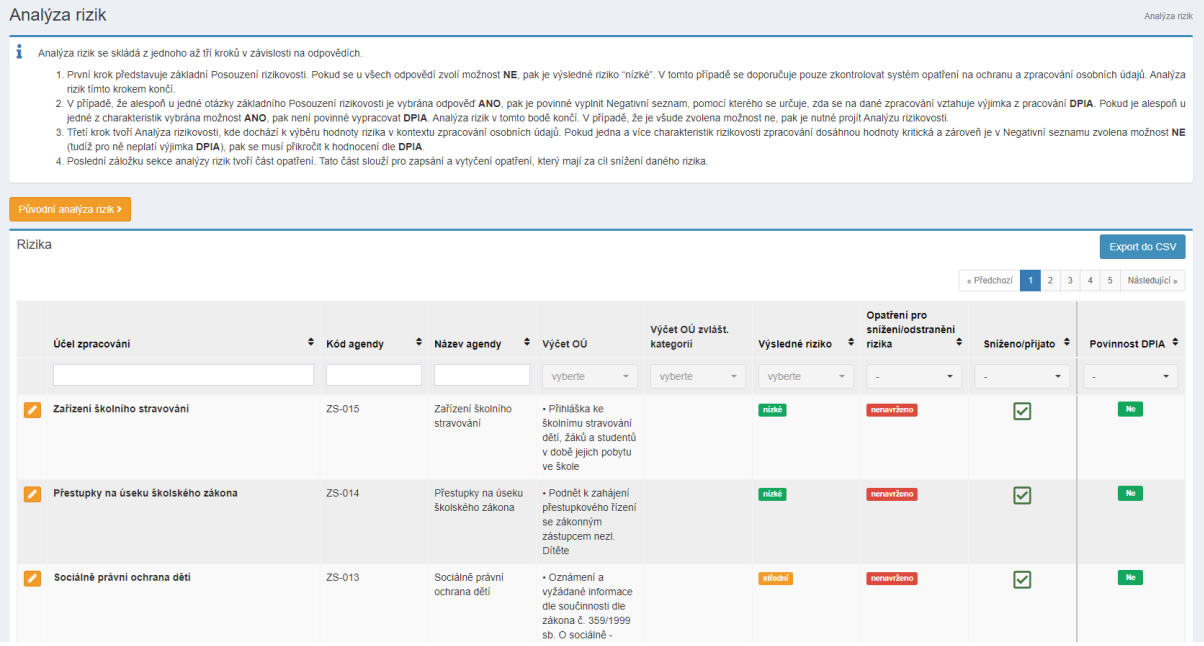
Analýza rizik se skládá z jednoho až tří kroků v závislosti na odpovědích.

První krok představuje základní Posouzení rizikovosti. Pokud se u všech odpovědí zvolí možnost NE, pak je výsledné riziko "nízké". V tomto případě se doporučuje pouze zkontrolovat systém opatření na ochranu a zpracování osobních údajů. Analýza rizik tímto krokem končí.

V případě, že alespoň u jedné otázky základního Posouzení rizikovosti je vybrána odpověď ANO, pak je povinné vyplnit Negativní seznam, pomocí kterého se určuje, zda se na dané zpracování vztahuje výjimka z pracování DPIA. Pokud je alespoň u jedné z charakteristik vybrána možnost ANO, pak není povinné vypracovat DPIA. Analýza rizik v tomto bodě končí. V případě, že je všude zvolena možnost ne, pak je nutné projít Analýzu rizikovosti.

Třetí krok tvoří Analýza rizikovosti, kde dochází k výběru hodnoty rizika v kontextu zpracování osobních údajů. Pokud jedna a více charakteristik rizikovosti zpracování dosáhnou hodnoty kritická a zároveň je v Negativní seznamu zvolena možnost NE (tudíž pro ně neplatí výjimka DPIA), pak se musí přikročit k hodnocení dle DPIA.

Poslední záložku sekce analýzy rizik tvoří část opatření. Tato část slouží pro zapsání a vytyčení opatření, který mají za cíl snížení daného rizika.



Dále se ve vztahu k rizikům eviduje, zda bylo dané riziko sníženo opatřením nebo přijato. Změnu hodnoty tohoto atributu lze provést buď přímo v přehledu *Analýzy rizik* ve sloupci "Sníženo/přijato" zaškrtnutím pole u příslušného záznamu, nebo ve formuláři analýzy konkrétního rizika.

Změny ve formuláři analýzy rizika je vždy nutné potvrdit stisknutím funkce **Uložit**.

Také lze provádět analýzu rizik dle starší metodiky. A to pomocí funkce **Původní analýza rizik**. Tento postup **nedoporučujeme**, protože není dle současné metodiky správný. Mezi oběma typy analýz se lze přepínat prostřednictvím následujících funkcí:

Analýzu rizik lze exportovat do souboru .csv stisknutím funkce **Export do CSV**.

Shrnutí a závěr

Žáci během dvou vyučovacích hodin provedou inventarizaci a analýzu rizik alespoň tří zpracování osobních údajů. V rámci inventarizace si vyplní ke všem zpracováním vhodné atributy tak, aby co nejvíce připomínaly modelovou organizaci – základní školu. Při analýze rizik vyučující osvětlí žákům její jednotlivé kroky a jejich vliv na návrh a zavádění opatření. Na základě výsledků této práce v nástroji GDA zváží vyučující, zda žák pokročí do další, manažerské části, která představuje vrchol celé analýzy. Tato část bude rovněž vyučována za pomocí 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