SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 37570/2023-SŽ-GŘ-O8
Listů/příloh 3/1

Vyřizuje Miriam Hemzová
Mobil 601 131 781
E-mail Hemzova@spravazeleznic.cz

Datum 02. 06. 2023

**Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem *„Prevence úniku dat"***

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen *„Zadavatel"*) Vás touto cestou informuje o tom, že připravuje zadávací řízení na veřejnou zakázku *„Prevence úniku dat"*. Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen *„PTK"*), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení a způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude:

- zajištění přípravy na nasazení nástroje Microsoft Purview DLP a jeho implementace pro oblast Microsoft služeb používaných v prostředí Zadavatele,
- analýza prostředí, vytvoření strategie a implementace souboru bezpečnostních opatření pro prevenci úniku dat nad vybranými non-Microsoft systémy Zadavatele.

Předmětem PTK bude zejména diskuze o níže uvedených tématech. Výčet témat je pouze demonstrativní a může být Zadavatelem rozšířen nebo zúžen kdykoliv před konáním PTK nebo i v průběhu PTK samotné, vyplyne-li tato potřeba z průběhu PTK. Zájmem Zadavatele je získat, co nejkomplexnější a nejucelenější soubor informací, které jsou pro vyhlášení předmětné veřejné zakázky nezbytné a žádoucí.

Okruh témat a dotazů:

1. **Specifikace předmětu plnění a nastavení jeho rozsahu, etap, dílčích kroků, nastavení parametrů poptávaných služeb, vhodnost rozdělení plnění na analyticko-přípravnou a implementační část.**
2. **Doba potřebná k realizaci předmětu plnění.**
3. **Předpokládaná hodnota veřejné zakázky, dostatečnost podkladů nezbytných pro stanovení nabídkové ceny (resp. nacenění).**

PTK je podle Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. 2. 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES a podle § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen *„Zákon"*) možností zadavatele předtím, než vyhlásí veřejnou zakázku, přičemž zadavatel má možnost v rámci PTK komunikovat s dodavateli (případně dalšími relevantními osobami) s cílem připravit zadání veřejné zakázky a informovat hospodářské subjekty (resp. dodavatele) o svých plánech a požadavcích při zadávání veřejných zakázek – zadavatel přitom může v rámci PTK i zjišťovat možnosti dodavatelů a případně i jejich návrhy řešení.



Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

**Generální ředitelství**
**Dlážděná 1003/7**
**110 00 Praha 1**

V rámci PTK bude představen nejprve záměr Zadavatele, včetně některých navrhovaných detailů, které se týkají, jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé pak budou mít možnost se k navrhovaným parametrům veřejné zakázky vyjádřit. Tímto postupem dojde ke zvýšení transparentnosti zadávacího řízení a k získání relevantních a objektivních informací o možnostech trhu, tak aby mohl Zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení.

**Forma PTK:** písemná, případně ústní

**Způsob konání PTK:**

1. **Fáze**: Zadavatel v rámci této pozvánky a její přílohy obeznamuje potenciální účastníky PTK se svým záměrem a potřebami. Zadavatel touto PTK cílí zejména na potenciální dodavatele působící na relevantním trhu. Za tímto účelem Zadavatel předkládá jako přílohu této pozvánky, aktuální bližší specifikaci připravované veřejné zakázky. Dodavatelé, kteří po prostudování poskytnuté specifikace budou mít zájem o další účast na PTK, potvrdí Zadavateli svou účast na email a v termínu uvedeném níže. Zadavatel má zájem o co nejširší účast na PTK, a proto v případě, že dodavatel projeví svůj zájem opožděně, Zadavatel takového dodavatele zahrne do procesu PTK. To neplatí v případě, že to již nebude technicky možné či vzhledem k pokročilosti procesu PTK vhodné.
2. **Fáze**: Dodavatelům, kteří na základě pozvánky zveřejněné Zadavatelem potvrdí ve stanovené lhůtě svůj zájem o účast na PTK, budou ze strany Zadavatele zaslány dokumenty: specifikace předmětu plnění, informace k systémům SŽ a dotazy k nabízenému řešení, a to prostřednictvím e-mailu, na emailovou adresu kontaktní osoby dodavatele. Tuto osobu určí dodavatel a v rámci potvrzení své účasti sdělí její kontaktní údaje. Dotazy budou zaslány nejpozději do 7 dnů od ukončení registrace.
3. **Fáze**: Odpovědi, které obdrží Zadavatel od dodavatelů ve lhůtě, která bude dodavatelům sdělena společně s konkrétními dotazy, budou Zadavatelem pečlivě analyzovány a vyhodnoceny. S ohledem na účel PTK Zadavatel přihlédne i k opožděným odpovědím, bude-li to možné a vhodné pro účel PTK. Zadavatel však žádá účastníky, aby stanovené termíny dodrželi. Dojde-li Zadavatel k závěru, že některá témata zůstávají nadále nejasná, sporná či vyvstane potřeba objasnění dalších doplňujících dotazů, přistoupí Zadavatel ke konání dalšího kola PTK, které bude uskutečněno nejspíše opět písemnou formou prostřednictvím e-mailu, Zadavatel si však vyhrazuje možnost požádat zástupce dodavatelů o realizaci prezenčního jednání. Tento postup bude Zadavatelem opakován, dokud nebudou obdrženy veškeré informace potřebné ke správnému nastavení parametrů veřejné zakázky s názvem „Prevence úniku dat". Zadavatel o dalším průběhu PTK osloví vždy minimálně ty dodavatele, kteří projevili zájem o PTK v předcházejícím kole.

Pro bližší informace ohledně PTK se lze obrátit na tento email:

**email:** **cnitptk@spravazeleznic.cz**

Zadavatel sděluje, že připravovaná veřejná zakázka je plánována k zadání jako nadlimitní sektorová veřejná zakázka.

Předpokládaný počátek plnění předmětu veřejné zakázky je 1. kvartál roku 2024. Předpokládaná délka trvání veřejné zakázky je 12 měsíců, přičemž tato délka může být na základě realizované PTK upravena.

V případě Vašeho zájmu o účast na této PTK potvrďte, prosím, Vaši účast na emailovou adresu: cnitptk@spravazeleznic.cz, **a to nejpozději do 12. 06. 2023.**

Dodavatel by ve výše uvedeném potvrzení měl uvést minimálně:

- název dodavatele a sídlo dodavatele;
- IČO dodavatele;
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail).

PTK nesmí vést k porušení základních zásad Zákona. Průběh i výsledek PTK proto bude zaznamenán ve zprávě vytvořené Zadavatelem. Informace z PTK užité v zadávacích podmínkách veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na PTK podílely. Zadavatel současně uvede v zadávacích podmínkách i všechny podstatné informace, které byly obsahem PTK a ovlivnily nastavení zadávacích podmínek.

Děkuji za spolupráci.

S pozdravem

Ing. David Miklas
02.06.2023 10:29
Podepsáno elektronicky

**Ing. David Miklas**
ředitel Správy železniční telematiky

**Přílohy:**
Příloha č.1 – Specifikace předmětu plnění

# Příloha 1 - Specifikace předmětu plnění

# Předběžná tržní konzultace k projektu Prevence úniku dat

Správa železnic, státní organizace (dále jen „*SŽ*“) plánuje implementaci řešení pro prevenci úniku dat ve vybraných systémech a aplikacích ICT prostředí SŽ. Cílem této předběžné tržní konzultace (dále jen „PTK“) je získání relevantních informací o možných nebo vhodných přístupech k ochraně dat a řešeních pro případné zadání jedné nebo více budoucích veřejných zakázek dostatečně přesným, technologicky neutrálním a nediskriminujícím způsobem a současně postupem, který bude vyhovovat požadavkům a prostředí SŽ.

Projekt je koncipován do dvou částí, kterým se věnuje tato příloha PTK:

1) **Část 1 - Prevence úniku dat s využitím nástroje Microsoft Purview DLP**
   Jelikož SŽ disponuje licencemi pro rodinu produktů v rámci Microsoft 365 E5 P2 a F3 + F5, hodlá zadavatel využít nástroje Microsoft Purview DLP pro pokrytí maxima Microsoft služeb využívaných v prostředí SŽ. Předmětem této části je nasazení nástroje Microsoft Purview DLP a souvisejících služeb určených k prevenci úniku dat.

2) **Část 2 - Prevence úniku dat pro non-Microsoft prostředí**
   Pro aplikace a systémy, které nebude možné dostatečně chránit před únikem dat pomocí nástroje Microsoft Purview DLP, předpokládáme využití dalších doporučených postupů a/nebo technologií pro zajištění prevence úniku dat. Předmětem této části je stanovení strategie prevence úniku dat, výběr a implementace odpovídajících postupů a/nebo technických nástrojů.

***Uchazeči o předběžnou tržní konzultaci se mohou účastnit pouze jedné části PTK.***


Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.spravazeleznic.cz

**Generální ředitelství**
**Dlážděná 1003/7**
**110 00 Praha 1**

# Část 1 - Prevence úniku dat s využitím nástroje Microsoft Purview DLP

SŽ aktuálně disponuje platformou M365 s možností využít řešení Microsoft Purview DLP, které nabízí funkcionalitu pro prevenci úniku dat určenou zejména pro prostředí Microsoft služeb a preferuje jeho využití u systémů SŽ všude, kde je to možné.

Nasazení a provoz služeb Microsoft Azure včetně Microsoft 365, nastavení prostředí do souladu s platnými interními předpisy, legislativou a dle aktuálních bezpečnostních a provozních doporučení s předáním znalostí internímu týmu je předpokladem pro úspěšné nasazení a provozování platformy Microsoft Purview DLP.

Zadavatel si je vědom, že toto řešení nezajistí plnohodnotnou ochranu všech aplikací a systémů SŽ mimo prostředí Microsoft služeb. Požadavky pro zajištění prevence úniku dat v těchto non-Microsoft prostředích je popsáno v druhé části této přílohy PTK (Prevence úniku dat pro non-Microsoft prostředí). Oba projekty sdílí cíl prevence úniku citlivých dat s rozdílem ve vymezení pokrytých systémů a prostředí.

## Hlavní cíle projektu

- Snížení rizik v souvislostí s narušením parametru důvěrnosti.
- Naplnění legislativních požadavků v kontextu ochrany citlivých dat v klíčových systémech.
- Automatizovaný přístup k detekci a zamezení úniku citlivých dat.
- Definování a nastavení způsobu reportingu detekovaných událostí, řešení incidentů a způsob úpravy detekčních a blokovacích pravidel.
- Maximální využití disponibilního portfolia Microsoft nástrojů v oblasti Data Protection v prostředí SŽ pro plnohodnotné nasazení Purview DLP.
- Vytvoření metodického postupu a technického předpisu k dosažení požadovaných změn – implementační plán a poté jeho realizace.
- Předání know-how ohledně správy a konfigurace na interní tým SŽ pro správu řešení a politik, které vyžadují detailní znalost interního prostředí a pravidel pro nakládání s citlivými údaji.
- Definovaná detekční pravidla a politiky budou svým přístupem minimalizovat invazivní zásahy do činnosti uživatelů a systémů při dodržení zásad ochrany informací.
- Nastavení a nasazení celkového systému pro systematickou a kontinuální ochranu dat v celém životním cyklu dat od jejich tvorby až po odstranění ze systému.

## Záměr projektu

**Požadavky na řešení**
Pro naplnění projektu uvažujeme o nasazení řešení na následující prostředí v SŽ:

1. Microsoft 365 E5 služby (Exchange Online, Sharepoint Online, OneDrive accounts, Teams, Defender for Cloud Apps).
2. Exchange (on premise/hybrid).
3. Koncové body Windows 10, Windows 11 a macOS.
4. On-premise file shares a on-premise SharePoint.

**Předpokládaný postup projektu**
K zajištění ochrany prostřednictvím nástroje Microsoft Purview DLP a úspěšné implementaci předpokládáme následující základní členění do dvou etap:

1) Příprava implementačního plánu
2) Realizace implementačního plánu

Následující kroky mohou být upraveny uchazečem dle jeho zkušeností s obdobnými projekty.

**Předběžné vymezení Etapy 1 - Příprava implementačního plánu**
Ve fázi přípravy implementačního plánu předpokládáme následující kroky:

1) **Splnění předpokladů pro úspěšné nasazení Purview DLP**
   - Celková příprava prostředí Microsoft služeb a identifikace nezbytných technických, organizačních nebo licenčních prerekvizit.
   - Vytvoření Microsoft Purview účtu a aktivace produktu Microsoft Purview DLP.
2) **Vytvoření cílů a strategie ochrany**
   - Identifikace garantů aktiv a rolí určených pro součinnost při plnění projektu.
   - Stanovení cílů – compliance, ochrana osobních údajů a business kritických dat. Předpokládáme rozsah, který bude definován a upřesněn také dle:
     - možností vybraných Microsoft nástrojů v oblasti ochrany dat a
     - rozsahu a typu chráněných aktiv (citlivých dat).
   - Analýza a upřesnění počtu uživatelů pracujících s citlivými daty v Microsoft prostředích, u nichž bude třeba nasadit preventivní komponentu Endpoint data loss prevention na koncový bod.
   - Zohlednění charakteru práce uživatelů s daty ve vybraných systémech, způsob sdílení dat s externími subjekty a jejich spolupráce na projektech SŽ a z toho plynoucí dopad na DLP politiky, případně úpravu počtu licencí.
3) **Tvorba implementačního plánu** (kroky vedoucí k naplnění strategie)
   - Mapování počátečního a cílového stavu a kroků se stanovením:
     - prioritizace dat,
     - kategorizace a štítkování dat,
     - politik pro nakládání s citlivými daty a jejich vytvoření.
   - Identifikace funkčností a nástrojů v rámci Microsot Purview Information Protection, které budou aktivovány.
   - Způsob zjišťování citlivých položek (viz dále připojení zdrojů dat).
   - Plánování politik a pořadí, v jakém budou implementovány.
   - Přístup k přechodu z testování politik do fáze jejich vynucování.
   - Skupiny rolí pro compliance tým SŽ a mapování na požadované činnosti.
   - Stanovení způsobu proškolení koncových uživatelů / administrátorů, osnova školení.
   - Stanovení způsobu testování a ladění politik.
   - Stanovení způsobu kontroly a aktualizace strategie ochrany před únikem dat na základě měnících se regulatorních, právních, oborových norem nebo pravidel ochrany duševního vlastnictví a obchodních potřeb relevantních pro prostředí SŽ.

**Předběžné vymezení Etapy 2 - Realizace implementačního plánu**
Ve fázi realizace implementačního plánu předpokládáme následující kroky vedoucí k naplnění vytvořené strategie:

1) **Konfigurace služby Microsoft Purview DLP** – nastavení pravidel klasifikace, definování typů citlivých informací a konfigurace notifikací v případě nalezení citlivých dat.
   a. Nastavení kategorie citlivých dat.
   b. Nastavení zakázaných a povolených činností s aktivy.
2) **Připojení zdrojů dat za účelem poznání dat** – skenování dat a citlivých informací on premise systémů. Identifikace zdrojů dat připojitelných do Purview DLP pro zjištění výskytu citlivých dat, definování zásad kontroly a jejich naplánování.
   a. Identifikace citlivých dat (využití definovaných typů citlivých dat, trénovatelných klasifikátorů).
   b. Datová klasifikace (využití content explorer).

   Předpokládáme využití služby Microsoft Purview Information Protection a skenování on premise zdrojů dat (úložiště) pro poznání typů dat na úložištích jako výchozí předpoklad pro další kroky a definice pravidel pro prevenci.

3) **Kontrola a náprava nálezů** – kontrola sestav nalezených citlivých informacích a realizace kroků k nápravě všech nalezených problémů, jako např. šifrování nebo odstranění citlivých dat.
4) **Příprava prostředí a nastavení ochranných akcí** (omezení přístupů, vizuální značky…) a souvisejících reakcí dle implementačního plánu:
   a. štítkování v office aplikacích a Windows,
   b. šifrování (emailové zprávy, přílohy),

c. identifikace, labeling a ochrana citlivých informací, které se nacházejí v on premise úložištích dat (Exchange, Sharepoint).

5) **Prevence úniku dat** – zabránění náhodnému a nadměrnému sdílení citlivých informací, nastavení detekčních pravidel a DLP politik. Příklady uvažovaných oblastí: Purview DLP on premise scanner, ochrana koncových bodů, rozšíření DLP funkčnosti pro prohlížeče, rozšíření monitorování aktivit se soubory a aplikování ochranných akcí pro tyto soubory na on premise sdílených složkách, Sharepoint složkách a knihovnách, ochrana Teams kanálů a zpráv.
6) **Konfigurace prostředí pro odbavování incidentů** (upozornění správce, reakce na incident a stavy incidentů, nastavení toku práce s incidentem).
7) **Testovací provoz s politikami v auditním módu**
8) **Školení uživatelů a administrátorů**
9) **Přechod do „enforcement" módu** (aktivního vynucování politik v prostředí SŽ).
10) **Monitorování a kontinuální údržba Purview DLP – pravidelné** používání Purview DLP v režimu interní správy SŽ. Očekáváme předání informací od dodavatele k zajištění efektivního fungování řešení, způsobu provádění nezbytných aktualizací klasifikačních pravidel a politik pro skenování nebo ladění politik.

# Část 2 - Prevence úniku dat pro non-Microsoft prostředí

SŽ disponuje velkým množstvím aplikací a systémů, jejichž data je třeba chránit před neoprávněným zneužitím nebo únikem. S ohledem na velikost organizace a velké množství různorodých aplikací, systémů a datových formátů, neplánuje SŽ implementaci postupů, konfigurací aplikací a/nebo využití DLP řešení pro všechna aktiva v jednom projektu, ale plánuje jejich postupné připojování podle technických a organizačních možností. V části Záměr projektu této přílohy PTK jsou uvedeny základní informace o předpokládaných krocích projektu nad vybranými systémy, které SŽ považuje v této části za prioritní a klíčové.

Pro tyto systémy, u nichž platforma Microsoft Purview DLP nedisponuje žádným mechanismem pro prevenci úniku dat je třeba definovat a následně implementovat takové bezpečnostní mechanismy, které povedou k minimalizaci úniků dat z těchto systémů a nebudou kolidovat s řešením Microsoft Purview DLP.

Prevence úniku dat je v kontextu této tržní konzultace definována jako soubor různých bezpečnostních opatření, konfiguračních postupů a/nebo technologií, které povedou k minimalizaci úniků dat z vybraných systémů. Tyto bezpečnostní postupy by měly zahrnovat i speciální úpravy provedené přímo ve vybraných systémech s využitím jejich nativních funkcí nebo prvků ICT infrastruktury SŽ. Prevenci úniku dat lze považovat za efektivní, pokud se postupuje na základě konceptu hloubkové ochrany. V této oblasti považujeme za klíčové například řízení přístupových oprávnění, vhodně nastavené politiky sdílení dat s externími subjekty, nastavení nejmenších oprávnění nebo klasifikační schémata. Nejedná se tedy pouze a výhradně o technologii typu DLP (Data Loss Prevention), která může být jednou z částí konceptu bezpečnostních opatření vedoucích k prevenci úniku dat.

## Hlavní cíle projektu

Cílem projektu je příprava strategie a vytvoření koncepce ochrany dat vybraných systémů a aplikací organizace jako předpokladu pro následnou implementaci technologických řešení, procesů nebo změn, které minimalizují rizika úniku dat (odtud níže navržené etapy projektu Strategie prevence úniku dat a Implementace bezpečnostních opatření určených k prevenci úniku dat).

**Hlavní cíle projektu:**

- Definice strategie ochrany na základě klasifikace dat SŽ, analýza a identifikace vektorů úniků dat z vybraných aplikací a systémů, revize bezpečnostních opatření k zamezení úniku dat na úrovni jednotlivých systémů.
- Vytvoření metodického postupu a technického zadání k dosažení požadovaných změn s využitím stávajících nebo doplnění nových technických a infrastrukturních prostředků, které umožní dosáhnout optimální úrovně prevence úniku dat.
- Nastavení ICT prostředí dle závěrů a cílů vytvořené koncepce tak, aby byly aktivovány preventivní mechanismy proti ztrátě dat.
- Definovaná detekční pravidla a politiky budou svým přístupem minimalizovat invazivní zásahy do činnosti uživatelů a systémů bez zásadního vlivu na kapacitu přenosu sítě a při dodržení zásad ochrany informací.
- Nasazení a nastavení celkového systému pro kontinuální ochranu dat v celém životním cyklu dat od jejich tvorby až po odstranění ze systému.
- Stanovení vhodné synergie nově definovaných ochranných mechanismů pro non-MS prostředí a stávajících nástrojů v SŽ (např. Purview DLP), aby nedocházelo ke vzájemným kolizím a nežádoucím překryvům či potřebě nadměrného úsilí při správě řešení.
- Implementace dalších kompenzačních technických opatření prevence úniku dat, která pokryjí neošetřené vektory.
- Definování a nastavení způsobu reportingu detekovaných událostí, řešení incidentů a způsob úpravy detekčních a blokovacích pravidel se zohledněním dostupných nástrojů SŽ.
- Automatizovaný přístup k detekci a zamezení úniku dat.
- Zvýšení bezpečnosti a plnění legislativních požadavků v kontextu ochrany citlivých údajů ve vybraných systémech.

## Záměr projektu

S ohledem na rozsah projektu a nutnosti úvodní přípravy prostředí, zejména po stránce organizace, rolí, odpovědností a vybraných aplikačních systémů, předpokládá SŽ rozdělení projektu na dvě na sebe navazující etapy:

- **Etapa 1 „Strategie prevence úniku dat"**– přípravná a analytická etapa vedoucí k definici celkové koncepce ochrany dat a vhodných postupů v souladu se stávajícím technickým prostředím SŽ.
- **Etapa 2 „Implementace principu DLP"** – výběr a implementace doporučených změn v aplikacích a systémech a/nebo technologií a jejich implementace do prostředí SŽ.

**Předběžné vymezení Etapy 1 – Strategie prevence úniku dat**

V rámci Etapy 1 SŽ předpokládá provedení následujících činností:

- Identifikace a monitoring datového prostředí u vybraných systémů, sběr informací o toku a charakteru dat z/do vybraných systémů pro získání přehledu o reálném využívání citlivých dat.
- Stanovení rozsahu a kategorií dat dle klasifikačního schématu SŽ, která budou předmětem ochrany a která budou podléhat pravidlům nakládání s daty.
- Analýza vektorů úniků dat a souvisejícího kybernetického ohrožení parametru důvěrnosti u vybraných aplikací a systémů.
- Vytvoření strategie a koncepce ochrany dat vybraných systémů s vrcholově definovanými politikami a pravidly pro nakládání s daty, která formují požadovanou ochranu dat (povolené a zakázané akce s daty).
- Identifikace a specifikace (předpis):
  - konkrétních bezpečnostních opatření v rámci konfiguračních možností jednotlivých systémů či ICT infrastruktury, která povedou k prevenci úniků dat, případně,
  - funkčností cílového DLP řešení, pokud bude potřeba,
  - upřesnění počtu uživatelů přistupujících k vybraným systémům a pracujících s citlivými dokumenty, což bude vstupní informací pro úpravu počtu licencí Microsoft Purview DLP na koncových bodech (Endpoint data loss prevention).
- Zohlednění stávajících nástrojů SŽ umožňujících realizovat v rámci některého vektoru prevenci úniku dat a specifikaci způsobu jejich začlenění do strategie ochrany.
- Stanovení procesu vypořádání DLP incidentů v prostředí SŽ a metodický způsob pro jejich zvládání, konfigurace politik.
- Návrh harmonogramu průběhu Etapy 2 a způsobu aktivace ochranných mechanismů aplikací a/nebo napojení cílových systémů do nově identifikovaného DLP řešení (nebo jeho součásti).
- Identifikace požadavků na součinnost a nezbytné vyčlenění kapacit SŽ při realizaci Etapy 2.

**Předběžné vymezení Etapy 2 – Implementace principu DLP**

Etapa 2 bude navazovat na předchozí etapu projektu a využije její výstupy. V Etapě 2 SŽ předpokládá zejména:

- Výběr a aktivace konkrétních preventivních ochranných mechanismů ve vybraných systémech či ICT infrastruktuře (např. nastavení oprávnění a přístupů, šifrování, konfigurace aplikačních auditing pravidel a reporting událostí a jejich retence, maskování dat v databázích, změna pravidel síťových komunikací, vystavených rozhraní a podobně).
- Výběr technologie DLP s požadavky dle výstupů Etapy 1 v případě nemožnosti zajistit dostatečně prevenci úniku dat nástroji a postupy uvedenými v předchozím bodě.
- Implementaci a konfiguraci vybraného systému DLP (pravidla, politiky, proces správy incidentů, role) k zajištění nepokrytých vektorů, např. Network DLP nepokryté v rámci Microsoft Purview DLP.

## Konkrétní oblasti a otázky, které jsou předmětem předběžné tržní konzultace

Bližší specifikace konkrétních oblastí a otázek ke dvěma výše uvedeným částem budou zaslány pouze registrovaným účastníkům této předběžné tržní konzultace.

SŽ poskytne registrovaným účastníkům dokument s dotazy a informacemi v následujících oblastech:

- **Specifikace předmětu plnění a nastavení jeho rozsahu, etap, dílčích kroků, nastavení parametrů poptávaných služeb, vhodnost rozdělení plnění na analyticko-přípravnou a implementační část.**
- **Doba potřebná k realizaci předmětu plnění.**
- **Předpokládaná hodnota veřejné zakázky, dostatečnost podkladů nezbytných pro stanovení nabídkové ceny (resp. nacenění).**