BEARCLAVE

Report z analýzy a plán klasifikace

Microsoft Purview — klasifikace dat a ochrana před únikem

Verze	1.0
Zpracoval	Bearclave s.r.o.
Klasifikace	Veřejné — vzorový dokument

Bearclave s.r.o., Třešňová 916/16, Přímětice, 669 04 Znojmo
IČO 30007534 · DIČ CZ30007534 · zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 153837
info@bearclave.cz · bearclave.cz

1. Manažerské shrnutí

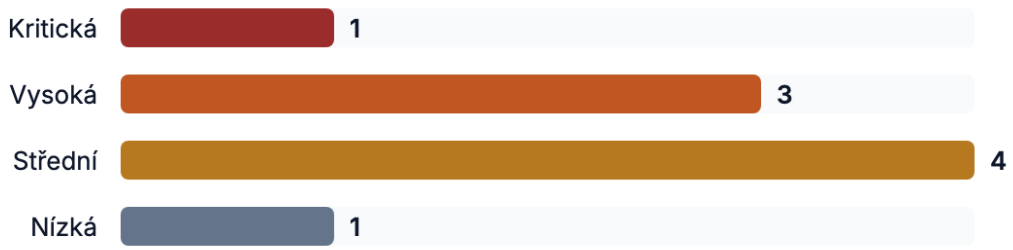
2 %	51	38 %	8 týdnů
dokumentů nese štítek	odkazů pro kohokoli na rodná čísla	shod rodného čísla je jiné číslo	pilot před prvním blokováním

Organizace má štítky citlivosti i pravidla proti úniku dat (DLP), ale nepoužívá je. Štítek nese kolem 2 % dokumentů a DLP běží od roku 2022 jen v režimu testu. Chybí výchozí štítek, popis, co kam patří, a rozhodnutí byznysu.

Nejnaléhavější je sdílení odkazem, který otevře kdokoli bez přihlášení. Na soubory s rodnými čísly pacientů jich vede 51, z toho 23 na hromadné exporty. Doporučujeme je uzavřít hned; zda jde o porušení s povinností ohlášení, posoudí pověřenec pro ochranu osobních údajů.

Nový plán má čtyři úrovně a funguje s dnešní licencí E3. Blokovat se začne až po osmitýdenním pilotu a jen tam, kde to data podpoří. Doplněk E5 Compliance pro 46 lidí, od kterých pochází 81 % souborů s rodnými čísly, je varianta k rozhodnutí vedení.

Nálezy podle priority



2. Rozsah a metoda

Prostředí	Hodnota
Organizace	síť 12 soukromých ambulancí
Uživatelé a licence	380 uživatelů, Microsoft 365 E3, bez doplňku E5 Compliance
Úložiště	64 webů SharePointu (41 s týmem), 380 OneDrivů, 22 sdílených schránek
Zdravotní dokumentace	odborný ambulantní systém mimo Microsoft 365, v rozsahu je to, co z něj odchází: exporty, žádanky, výpisy a korespondence
Ochrana dnes	štítky citlivosti publikované všem, jedna politika DLP v režimu testu

Analýza pokrývala štítky a jejich používání, licenční možnosti, výskyt rodných čísel v SharePointu, OneDrivu a Exchange, stávající DLP a nastavení sdílení mimo organizaci. Součástí byl dvouhodinový workshop s vedením, na kterém se rozhodlo, co je v organizaci citlivé. V prostředí se nic neměnilo.

2.1 Proti čemu se měřilo

- Objektivní data: auditní záznam za 90 dní (nastavení štítků, vytvoření a použití odkazů pro kohokoli), shody stávající DLP za 90 dní a nastavení prostředí.
- Posouzení v kontextu: rozhovory s vedoucími tří ambulancí a s fakturací, ruční kontrola vzorku 200 shod s pověřencem pro ochranu osobních údajů. Vzorek se procházel v prostředí organizace a data ho neopustila.
- Rozhodnutí vedení z workshopu: co je citlivé a kdo k tomu smí. Report je zapisuje, nenahrazuje.

2.2 Co analýza není

- Právní posouzení nakládání se zdravotními údaji ani posouzení, zda je některý nález porušením zabezpečení s povinností ohlášení.
- Posouzení odborného ambulantního systému a dalších systémů mimo Microsoft 365.
- Návrh retenčních lhůt.
- Implementace — plán je popsaný v kapitolách Plán klasifikace a Roadmapa.

3. Plán klasifikace

Plán vznikl na workshopu s vedením a stojí na jeho rozhodnutích. Je to zadání pro implementaci: co se nastaví, kde, v jakém pořadí a podle čeho se rozhodne o blokování.

3.1 Úrovně klasifikace

Čtyři úrovně bez podštítků



Štítek	Kdy použít	Ochrana	Kdo přistoupí
Veřejné	Informace pro pacienty, ceníky, texty na web, inzeráty	Žádná	Kdokoli
Interní	Rozpisy služeb, provozní pokyny, zápisy z porad. Výchozí pro nové dokumenty a e-maily	Bez značení a bez omezení	Zaměstnanci, partneři podle potřeby
Citlivé	Osobní údaje zaměstnanců, mzdy, smlouvy, finance	Zápatí, upozornění při sdílení mimo organizaci	Kdo s daty pracuje, mimo organizaci jen konkrétní lidé
Vysoce citlivé	Cokoli o konkrétním pacientovi: exporty, výpisy, žádanky, lékařské zprávy	Záhlaví, vodoznak, DLP, šifrování se rozhodne po pilotu	Kdo pacienty ošetřuje nebo administruje, ven jen šifrovaně

- Nové dokumenty a e-maily dostanou výchozí štítek Interní. Exporty z odborného systému, typicky CSV nebo PDF, ho nedostanou a chrání je pravidla podle obsahu.
- Snížení nebo odebrání štítku vyžaduje odůvodnění a zapíše se do auditního záznamu.
- Podštítky po odděleních nejsou. Kdo k čemu smí, řeší oprávnění webů a týmů.

3.2 Před čím se chrání

Starší dokumenty bez štítku tvoří 98 % obsahu a automatické štítkování licence E3 nepokrývá. Chrání je proto pravidla DLP s vlastním typem pro rodné číslo z nálezu N-003. Štítek chrání, co lidé označí sami, třeba lékařskou zprávu jen se jménem pacienta.

Podmínka	Kde	V pilotu	Po vyhodnocení
Rodné číslo 1 až 9krát nebo štítek Vysoce citlivé	E-mail mimo organizaci	Upozornit odesílatele	Zašifrovat automaticky
Rodné číslo 10krát a víc	E-mail mimo organizaci	Upozornit, hlášení správci	Blokovat, partnerům jen šifrovaně
Rodné číslo 1 až 9krát nebo štítek Vysoce citlivé	Sdílení souborů mimo organizaci	Upozornit vlastníka	Blokovat, přepsání s odůvodněním
Rodné číslo 10krát a víc	Sdílení souborů mimo organizaci	Upozornit, hlášení správci	Blokovat bez přepsání
Štítek Citlivé	E-mail a sdílení mimo organizaci	Upozornit	Upozornit
Rodné číslo	USB, osobní cloudová úložiště	—	Jen s doplňkem E5 Compliance

> Hranice 10 výskytů odděluje hromadný export od korespondence o jednom pacientovi. Je to výchozí hodnota, pilot ji potvrdí nebo posune.

3.3 Rozsah platforem a pořadí

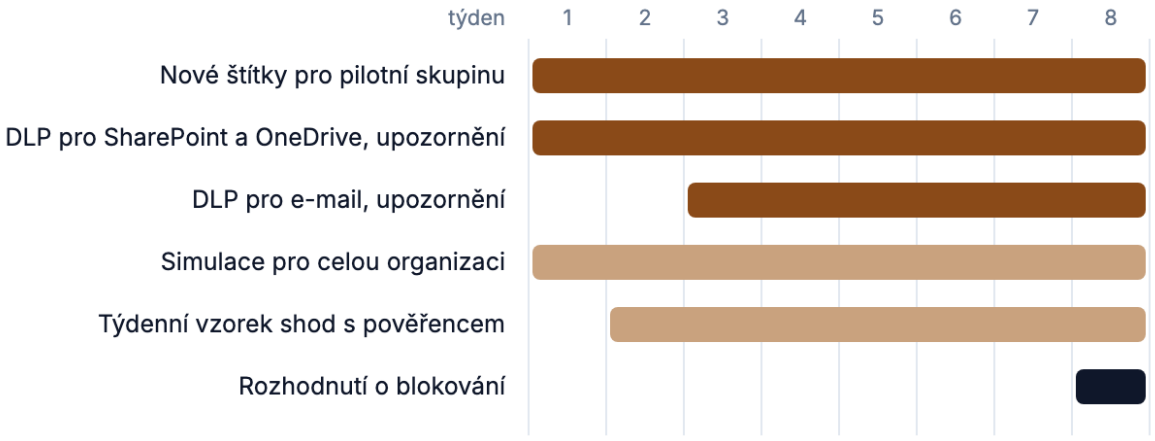
Platformy se zapínají postupně. Každá další přijde, až předchozí běží bez překvapení.

Pořadí	Platforma	Co se zapíná	Proč v tomto pořadí
1	SharePoint a OneDrive	Nové štítky, výchozí štítek, DLP pro sdílení mimo organizaci	7 700 souborů se shodou a nejvážnější nález, včetně souborů z Teams
2	Exchange	Výchozí štítek pro e-maily, DLP pro zprávy ven, šifrování	11 400 zpráv se shodou. Partneři potřebují náhradní cestu dřív, než se něco zablokuje
3	Týmy a weby	Štítky pro týmy a weby	Řídí soukromí, hosty a sdílení celého týmu
4	Koncová zařízení	Endpoint DLP pro USB a osobní úložiště	Jen s doplňkem E5 Compliance
—	Chat v Teams	—	Ověří se proti licenčním podmínkám, zatím se hlídají soubory

3.4 Pilot a přechod na blokování

Pilot trvá osm týdnů na 16 lidech ze tří ambulancí od recepce po lékaře, jmenovitě je určilo vedení. Stejná pravidla běží pro celou organizaci v režimu simulace: nikoho neomezí ani neupozorní, ale dají čísla za celou organizaci. Každý týden se měří shody, podíl planých shod ve vzorku s pověřencem, přepsání upozornění a legitimní toky ven.

Průběh pilotu (týdny)



3.4.1 Kritéria přechodu na blokování

- Pravidlo běželo v režimu upozornění aspoň 4 týdny.
- Plané shody ve vzorku jsou pod 10 %.
- Každý legitimní tok ven, který by blokace zastavila, má náhradní cestu: šifrovaný e-mail, sdílení s konkrétní osobou nebo schválenou výjimku pro partnera.
- Vlastník dotčeného procesu přechod odsouhlasil.

> Pravidlo, které kritéria nesplní, zůstane v režimu upozornění, upraví se a vyhodnotí znovu po dalších 4 týdnech.

4. Nálezy

Tři nálezy v plném znění. Ostatní jsou v registru nálezů v příloze.

4.1 N-001 — Štítky existují, ale nepoužívají se

Vlastnost	Hodnota
Oblast	Štítky
Priorita	**Vysoká**
Pracnost	Střední
Licence	E3 stačí

4.1.1 Zjištěný stav

Štítky citlivosti v prostředí jsou, ale nikdo neurčil, co do kterého patří, a byznys je nikdy neschválil. Popisy jsou prázdné a podštítky rozdělené po odděleních vidí kvůli jediné politice publikování všichni. Za 90 dní dostalo štítek kolem 2 % nově vytvořených nebo nahraných dokumentů.

Nové a nahrané dokumenty za 90 dní



4.1.2 Dopad

Organizace má klasifikaci na papíře, ne v datech. Pravidla, která by se o štítky opírala, nemají o co, a nový pokus nad stejnými štítky by dopadl stejně.

4.1.3 Doporučení

- Nahradit dnešní štítky čtyřmi úrovněmi bez podštítků podle kapitoly Plán klasifikace. Co do které patří, rozhodlo vedení na workshopu.

- Každému štítku dát popis s příklady z dokumentů organizace, který se zobrazí přímo v aplikaci.
- Staré štítky nemazat, po rozšíření do celé organizace je jen stáhnout z publikování. Dokumenty, které je nesou, zůstanou dostupné stejným lidem.

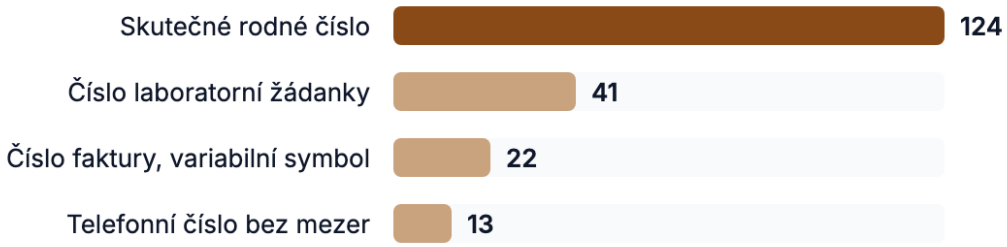
4.2 N-003 — Vestavěný typ pro rodné číslo hlásí jiná čísla a část rodných čísel míjí

Vlastnost	Hodnota
Oblast	Rozpoznávání
Priorita	**Vysoká**
Pracnost	Střední
Licence	E3 stačí, rozpoznávání textu ve skenech se ověří

4.2.1 Zjištěný stav

Stávající politika hledá rodná čísla vestavěným typem citlivé informace pro české rodné číslo. Ve vzorku 200 shod, který jsme prošli s pověřencem, bylo 76 jiných čísel, tedy 38 %. Z 50 dokumentů, o kterých pověřenec věděl, že rodná čísla obsahují, politika minula 11: sedm naskenovaných žádanek a čtyři s mezerou místo lomítka.

Vzorek 200 shod vestavěného typu



4.2.2 Dopad

Při 38 % planých shod by blokování zastavilo běžnou fakturaci a komunikaci s laboratořemi. Lidé by ochranu obcházeli a vedení by ji nakonec vypnulo.

4.2.3 Doporučení

- Vytvořit vlastní typ citlivé informace postavený na pravidlech tvorby rodného čísla. Desetimístná čísla přidělovaná od roku 1954 jsou dělitelná jedenácti, výjimkou jsou čísla se zbytkem 10 a kontrolní číslicí 0. K měsíci se u žen přičítá 50 a od roku 2004 v případě potřeby i 20.
- Devítimístná čísla z doby před rokem 1954 kontrolní číslici nemají. Hlásit je jen s klíčovým slovem v blízkosti, například rodné číslo, RČ, datum narození nebo číslo pojištěnce.
- Jak se kontrola nastaví v definici typu, ověřit a doladit na vzorku dat. Cíl je daný předem: na novém vzorku 200 shod méně než 10 % planých a žádné minuté rodné číslo s mezerou.
- Naskenované žádanky potřebují rozpoznávání textu v obrázcích. Jeho licenční a cenové podmínky se ověří, do té doby jsou skeny známá mezera.

4.3 N-004 — Soubory s rodnými čísly sdílené odkazem pro kohokoli

Vlastnost	Hodnota
Oblast	Sdílení
Priorita	**Kritická**
Pracnost	Nízká
Licence	E3 stačí

4.3.1 Zjištěný stav

SharePoint i OneDrive dovolují sdílet odkazem, který otevře kdokoli bez přihlášení. Je to výchozí typ odkazu, nevyprší a platných je dnes přes 4 900. Pověřenec ručně prošel 58 odkazů na soubory se shodou rodného čísla: 51 z nich vede na skutečná rodná čísla pacientů, 23 na hromadné exporty.

Ověření: nastavení sdílení v organizaci

```
Get-SPOTenant | Select-Object SharingCapability, OneDriveSharingCapability,
    DefaultSharingLinkType, RequireAnonymousLinksExpireInDays

SharingCapability                : ExternalUserAndGuestSharing
OneDriveSharingCapability        : ExternalUserAndGuestSharing
DefaultSharingLinkType           : AnonymousAccess
RequireAnonymousLinksExpireInDays : 0
```

4.3.2 Dopad

Kdo odkaz dostane, třeba přeposláním, otevře export se jmény, rodnými čísly a údaji o zdravotním stavu, a to bez přihlášení. Auditní záznam pak ukáže jen IP adresu, ne člověka.

4.3.3 Doporučení

- Seznam platných odkazů na soubory s rodnými čísly předat vlastníkům, aby legitimní sdílení poslali znovu konkrétní osobě.
- Vypnout odkazy pro kohokoli pro SharePoint i OneDrive a výchozí typ odkazu nastavit na konkrétní lidi. Dosavadní odkazy pro kohokoli přestanou fungovat.
- Materiály pro pacienty přesunout na veřejný web, na tom se vedení shodlo.
- Pověřenec posoudí, zda jde o porušení zabezpečení s povinností ohlášení.

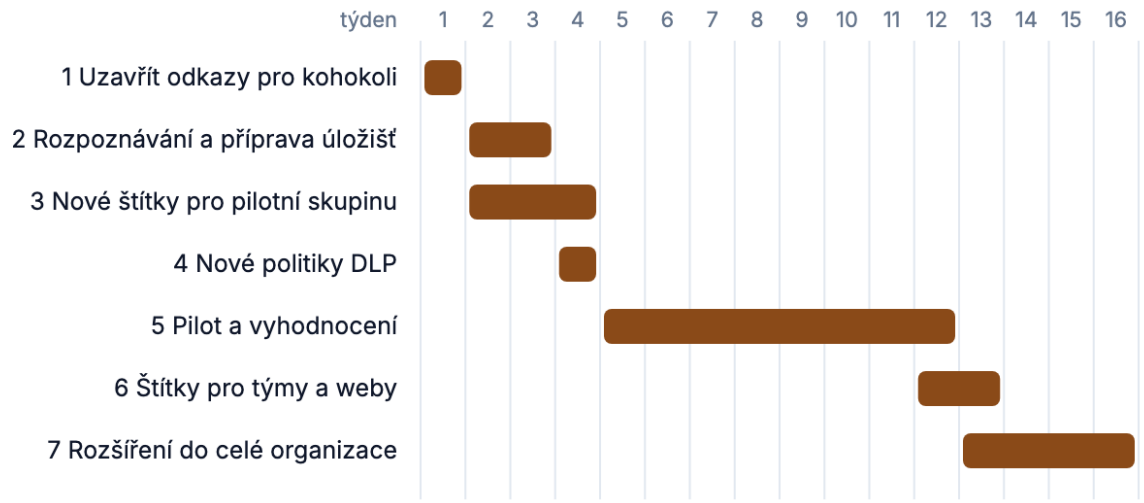
Sdílení ven jen s ověřenými lidmi

```
Set-SPOTenant -SharingCapability ExternalUserSharingOnly `
    -OneDriveSharingCapability ExternalUserSharingOnly `
    -DefaultSharingLinkType Direct
```

5. Roadmapa

Pořadí je podle rizika a závislostí: nejdřív se zavře, co uniká, pak se připraví rozpoznávání a štítky a teprve potom se zapínají pravidla. Kalendářně zhruba 16 týdnů, z toho 8 týdnů pilot.

Harmonogram (týdny)



Krok	Obsah	Nálezy	Pracnost
1	Vypnout odkazy pro kohokoli, seznam dotčených souborů předat vlastníkům	N-004	Nízká
2	Vlastní typ pro rodné číslo laděný na vzorku, podpora štítků v SharePointu a OneDrivu, přesměrování Plochy a Dokumentů do OneDrivu	N-003, N-007, N-009	Střední
3	Nové štítky s popisy a výchozím štítkem, publikování pilotní skupině	N-001, N-002	Střední
4	Nové politiky DLP v simulaci a s upozorněním, připravené šifrování, vypnutí staré politiky	N-005, N-008	Střední
5	Pilot, vyhodnocení a přechod na blokování po jednotlivých pravidlech	—	Střední
6	Štítky pro týmy a weby	N-006	Nízká
7	Rozšíření do celé organizace po ambulancích, stažení starých štítků z publikování	—	Střední

> Varianta s doplňkem E5 Compliance přidá krok pro koncová zařízení s vlastním pilotem. Konfigurace vzniká jako kód ve verzovaném repozitáři, každá změna jde přes schválení a dá se vrátit.

6. Přílohy

6.1 Registr nálezů

ID	Nález	Oblast	Priorita	Pracnost
N-001	Štítky se nepoužívají, označená jsou 2 % dokumentů	Štítky	Vysoká	Střední
N-002	Chybí výchozí štítek pro nové dokumenty a e-maily	Štítky	Střední	Nízká
N-003	Vestavěný typ rodného čísla hlásí jiná čísla, část míjí	Rozpoznávání	Vysoká	Střední
N-004	Rodná čísla sdílená odkazem pro kohokoli	Sdílení	Kritická	Nízká
N-005	DLP od roku 2022 v testu, hlášení nikdo nečte	DLP	Střední	Nízká
N-006	Týmy nemají štítky, 4 týmy s exporty mají 17 hostů	Štítky	Střední	Nízká
N-007	Podpora štítků v SharePointu a OneDrivu je vypnutá	Štítky	Nízká	Nízká
N-008	E-maily s rodnými čísly jdou ven nešifrované	E-mail	Vysoká	Střední
N-009	Exporty na discích a USB, kam DLP s E3 nedosáhne	Koncová zařízení	Střední	Střední

6.2 Licenční přehled

Funkce	E3	E5, E5 Compliance	V plánu
Ruční štítkování a výchozí štítek	Ano	Ano	Ano, základ plánu
Obsahové značení a šifrování štítkem	Ano	Ano	Šifrování po pilotu
Štítky pro týmy, skupiny a weby	Ano	Ano	Ano
Šifrování e-mailových zpráv	Ano	Ano	Ano, zprávy ven
DLP pro Exchange, SharePoint a OneDrive	Ano	Ano	Ano
Vlastní typy citlivých informací v DLP	Ano	Ano	Ano, rodné číslo
DLP pro zprávy v chatu Teams	Ověří se	Ano	Ověří se
Automatické štítkování na straně klienta i služby	Ne	Ano	Ne
Endpoint DLP	Ne	Ano	Varianta pro 46 lidí
Trénovatelné klasifikátory a EDM	Ne	Ano	Ne

> Stav licenčních podmínek k datu analýzy, před nákupem doplňku se ověří znovu. Rozpoznávání textu ve skenech má vlastní licenční a cenové podmínky.