

Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

Toto je 1. téma ze sedmidílné série.



Úvod

Toto řešení představuje možnosti ochrany citlivých dat uložených ve službách Office 365. Zahrnuje normativní doporučení, jak vyhledávat, kategorizovat, chránit a monitorovat osobní údaje. Jako příklad v něm používáme obecné nařízení o ochraně osobních údajů, stejný proces ale můžete uplatnit na cestě k dosažení shody s mnoha dalšími regulacemi.

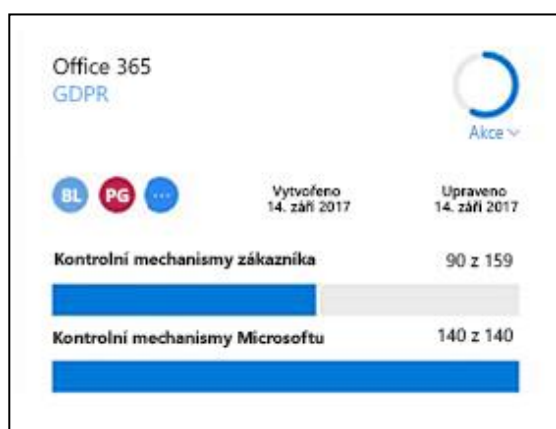
Nařízení GDPR upravuje shromažďování, ukládání, zpracování a sdílení osobních údajů. Ty jsou v něm – konkrétně ve článku 4 – definovány velmi široce jako jakékoli údaje související s identifikovanou nebo identifikovatelnou fyzickou osobou, která je rezidentem Evropské unie. Úplnou definici najdete v tématu 2.

Obsah tohoto řešení má organizacím pomoci s vyhledáváním a ochranou osobních údajů v Office 365, které mohou podléhat nařízení GDPR. Nenabízíme jej jako osvědčení o souladu s nařízením GDPR. Za zajištění této shody odpovídají organizace. Doporučujeme problematiku konzultovat s právním oddělením a týmy pro dodržování předpisů, případně se poradit s externími poskytovateli, kteří se na tuto oblast specializují.

Bezplatný nástroj pro posouzení souladu s nařízením GDPR nabízí možnost rychlého vlastního vyhodnocení online. Vaše organizace tak může posoudit celkovou úroveň své připravenosti na shodu s GDPR (<http://aka.ms/gdprassessment>).

Posuďte a řiďte rizika nedodržení předpisů

1 Pomocí služby Compliance Manager prohlížejte požadavky regulačních předpisů a sledujte jejich plnění



Služba Compliance Manager poskytuje nástroje ke sledování, implementaci a správě kontrolních mechanismů auditování, které vaši organizaci pomohou dosáhnout shody s různými normami, včetně nařízení GDPR.

Další informace najdete v tématu 7 v tomto průvodci – **Použití služby Compliance Manager na portálu Service Trust Portal**.

2 Pomocí Vyhledávání obsahu a typů citlivých informací můžete vyhledávat osobní údaje

Zmapujte ve vašem prostředí osobní údaje podléhající nařízení GDPR. Pomocí Vyhledávání obsahu a typů citlivých informací můžete:

- Zjišťovat a vykazovat místo uložení osobních údajů
- Optimalizovat typy citlivých údajů a další dotazy tak, abyste vyhledali veškeré osobní údaje ve vašem prostředí

Typy citlivých informací určují, jak bude automatizovaný proces rozpoznávat konkrétní typy informací, jako jsou čísla zdravotního pojištění nebo platebních karet.

Tento průvodce obsahuje sadu typů, kterou můžete využít jako odrazový můstek. Do budoucna připravujeme řadu dalších typů citlivých informací pro osobní údaje v zemích EU.

Další informace najdete v tématu 2 v tomto průvodci – **Vyhledávání osobních údajů**.

Kategorizace, ochrana a monitorování osobních údajů v Office 365 a dalších aplikacích SaaS

Některé funkce používané k ochraně informací v Office 365 lze využít také k ochraně citlivých dat v dalších aplikacích SaaS.

3 Rozhodněte se, jestli chcete vedle typů citlivých informací používat také popisky

Typy citlivých informací jsou formou kategorizace. S rozhodnutím, zda implementovat také popisky, vám pomůže téma 3 **Architektura schématu kategorizace osobních údajů**. Pokud popisky chcete použít, najdete informace v tématu 4 **Použití popisků osobních údajů v Office 365**.

Kategorizace

4 Ochrana osobních údajů v Office 365

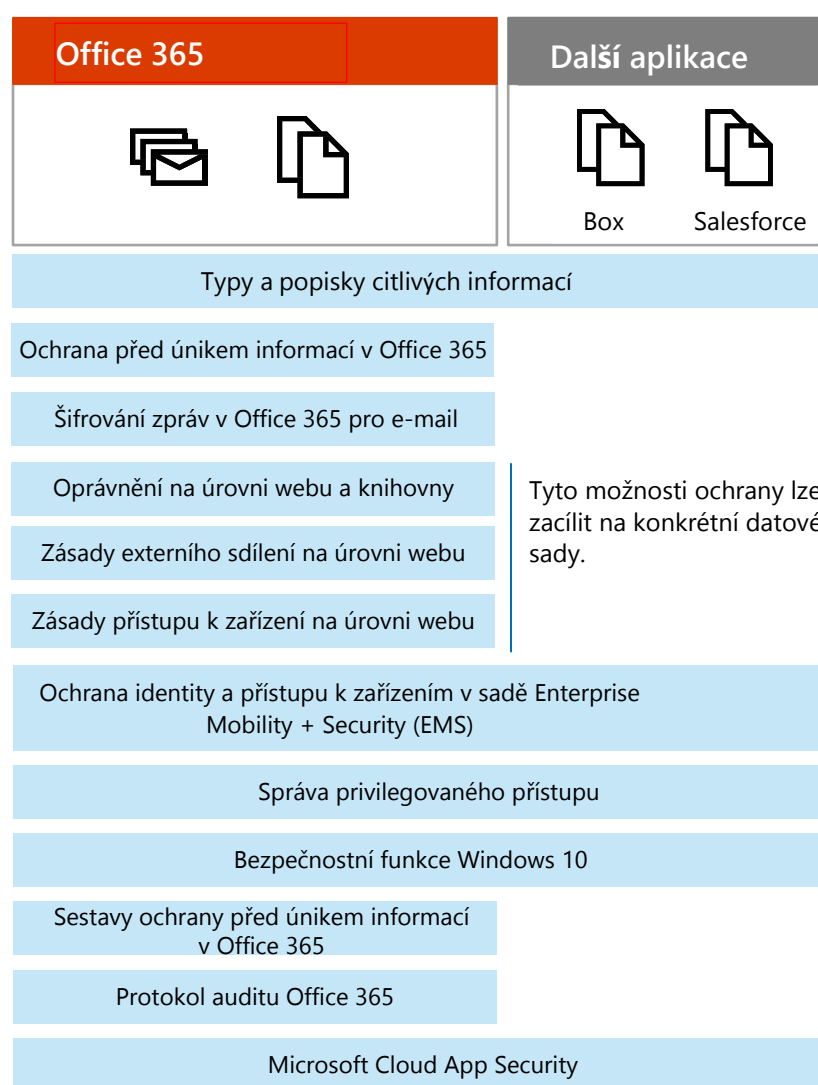
Další podrobnosti ke konfiguraci ochrany před únikem informací a k dalším možnostem ochrany citlivých dat najdete v tématu 5 **Použití ochrany citlivých dat v Office 365**.

Ochrana

5 Monitorování uniků osobních údajů

Sestavy ochrany před únikem informací v Office 365 nabízejí nejpodrobnější úroveň monitorování citlivých dat. Služba Cloud App Security rozšiřuje možnosti vyhledávání a monitorování těchto dat na další poskytovatele aplikací SaaS. Viz téma 6 **Monitorování průniků k osobním údajům**.

Monitorování



Připravujeme – použijte tyto možnosti spolu se službou Cloud App Security k vyhledání citlivých dat v dalších aplikacích SaaS.

Ochrana přístupu ke cloudovým službám

Další informace a materiály najdete v tématech 2–7

Prosinec 2017

© 2017 Microsoft Corporation. Všechna práva vyhrazena. Máte-li k této dokumentaci dotazy nebo připomínky, napište nám prosím na adresu CloudAdopt@microsoft.com.



Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

Toto je 2. téma ze sedmidílné série.



Vyhledání osobních údajů

Osobní údaje jsou v nařízení GDPR definovány velmi široce jako jakákoli data týkající se identifikované nebo identifikovatelné fyzické osoby, která je rezidentem Evropské unie.

Článek 4 – definice

„Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

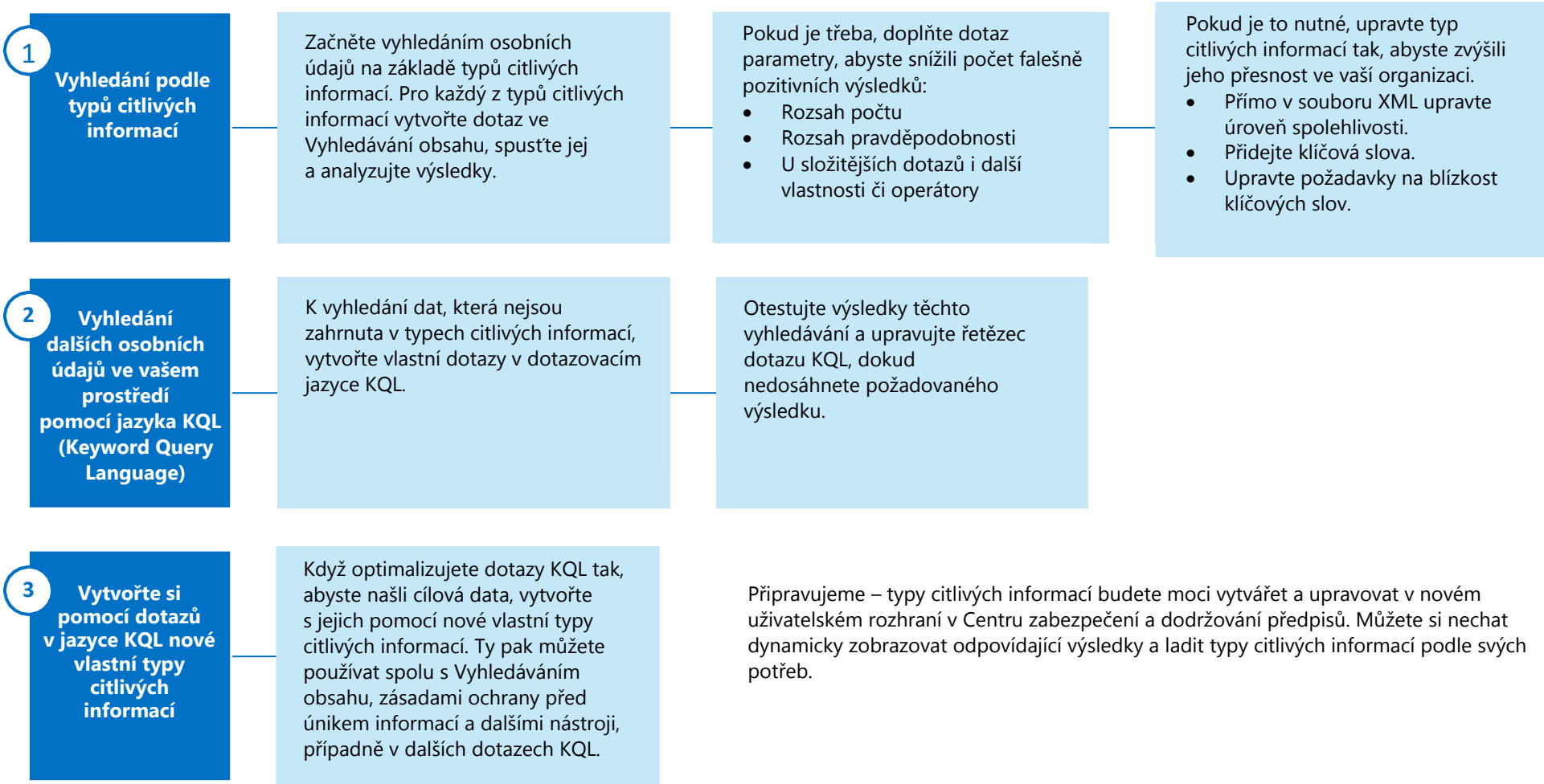
Toto téma ukazuje, jak vyhledat osobní údaje uložené ve službách SharePoint Online a OneDrive pro firmy (kam spadají i weby všech skupin Office 365 a weby ve službě Microsoft Teams).

Vyhledávání osobních údajů podléhajících nařízení GDPR v Office 365 probíhá na základě *typů citlivých informací*. Ty určují, jak bude automatizovaný proces rozpoznávat konkrétní typy informací, jako jsou čísla zdravotního pojištění nebo platebních karet. Momentálně je nelze využít k vyhledávání dat uložených v poštovních schránkách Exchange. Spolu se zásadami ochrany před únikem informací se typy citlivých informací nicméně dají použít k vyhledávání osobních údajů v poště během přenosu.

I když tedy v současné době nemůžete vyhledávat osobní údaje uložené ve schránkách v systému Exchange Online, můžete typy citlivých informací, které spravujete s ohledem na nařízení GDPR, využít k vyhledávání a ochraně osobních údajů v době, kdy jsou předávány e-mailem.

Vyhledávání osobních údajů pomocí Vyhledávání obsahu

Při vyhledávání osobních údajů v Office 365 doporučuje Microsoft trojfázový přístup. Ve zbývajících částech tohoto tématu vás jednotlivými fázemi provedeme.



Vyhledání typů citlivých informací pomocí Vyhledávání obsahu

S vyhledáváním osobních údajů začněte s využitím typů citlivých informací, které jsou součástí Office 365. Jsou uvedeny v Centru zabezpečení a dodržování předpisů v části Kategorizace.

Na následující stránce tohoto tématu je uveden seznam aktuálních typů citlivých informací vztahujících se na občany Evropské unie. Použijte je jako výchozí bod. Doporučujeme pravidelně sledovat nově přidané položky a podpořit tak zajištění shody s nařízením GDPR.

Viz také tento článek: [Seznam typů citlivých dat a údajů, které vyhledávají](#)

Typy citlivých informací

Určují, jak bude automatizovaný proces rozpoznávat konkrétní typy informací, jako jsou čísla bankovních účtů, zdravotního pojištění nebo platebních karet. Typy citlivých dat se označují také jako podmínky. Typ citlivých informací je definován vzorcem, který lze identifikovat pomocí regulárního výrazu nebo funkce. Vedle toho lze k rozpoznání typu citlivých informací využít podpůrné doklady, jako jsou klíčová slova a kontrolní součty. V procesu vyhodnocování se pracuje také s úrovní pravděpodobnosti a blízkostí.

Typy citlivých informací momentálně nelze použít k vyhledávání dat uložených v poštovních schránkách.

Použití Vyhledávání obsahu spolu s typy citlivých informací

<p>1 V Centru zabezpečení a dodržování předpisů přejděte na Vyhledávání obsahu.</p> <p>V levém podokně Centra zabezpečení a dodržování předpisů klikněte na Vyhledávání a prověřování > Vyhledávání obsahu.</p> <p>Spuštění Vyhledávání obsahu v Centru zabezpečení a dodržování předpisů Office 365</p>	<p>2 Vytvořte novou položku vyhledávání pro každý typ citlivých informací.</p> <p>Použijte následující syntaxi: <code>SensitiveType:"<type>"</code> Například: <code>SensitiveType:"France Passport Number"</code></p> <p>Jako rozsah vyhledávání použijte SharePoint (zahrnuje OneDrive pro firmy). Zkontrolujte přesnost syntaxe a ověřte, že jste nezadali nadbytečné mezery ani překlepy.</p> <p>Vytvoření dotazu k vyhledání citlivých dat uložených na webech</p>	<p>3 Prohlédněte si výsledky každého vyhledávání.</p> <p>Při posuzování přesnosti dotazu se zaměřte na tyto typy problémů:</p> <ul style="list-style-type: none"> Velký počet falešně pozitivních výsledků Chybějící známé instance dat <p>Export výsledků Vyhledávání obsahu z Centra zabezpečení a dodržování předpisů Office 365</p> <p>Poznámka: Pokud používáte prohlížeč Mozilla Firefox nebo Chrome, možná bude třeba sestavy poprvé stáhnout v prohlížeči Internet Explorer či Edge a nainstalovat požadovaný doplněk.</p>
---	---	---

Typy citlivých informací v údajích o občanech EU

Poznámka: Do budoucna připravujeme řadu dalších typů citlivých informací pro osobní údaje v zemích EU.

	Typ citlivých dat	Kategorie
Údaje o zákaznících	Číslo belgického národního identifikačního průkazu	Identifikovatelné osobní údaje (PII)
	Číslo platební karty	Osobní finanční údaje
	Číslo chorvatského identifikačního průkazu	Identifikovatelné osobní údaje (PII)
	Chorvatské osobní identifikační číslo (OIB)	Identifikovatelné osobní údaje (PII)
	Číslo českého občanského průkazu	Identifikovatelné osobní údaje (PII)
	Dánské osobní identifikační číslo	Identifikovatelné osobní údaje (PII)
	Číslo debetní karty EU	Osobní finanční údaje
	Finský národní identifikátor	Identifikovatelné osobní údaje (PII)
	Číslo finského pasu	Identifikovatelné osobní údaje (PII)
	Číslo francouzského řidičského průkazu	Identifikovatelné osobní údaje (PII)
	Národní identifikační karta (CNI) (Francie)	Identifikovatelné osobní údaje (PII)
	Číslo pasu (Francie)	Identifikovatelné osobní údaje (PII)
	Číslo sociálního zabezpečení (INSEE) (Francie)	Identifikovatelné osobní údaje (PII)
	Číslo německého řidičského průkazu	Identifikovatelné osobní údaje (PII)
	Číslo německého identifikačního průkazu	Identifikovatelné osobní údaje (PII)
	Číslo německého pasu	Identifikovatelné osobní údaje (PII)
	Řecký národní identifikační průkaz	Identifikovatelné osobní údaje (PII)
	Číslo IBAN	Osobní finanční údaje
	Adresa IP	Identifikovatelné osobní údaje (PII)
	Irské číslo PPS (Personal Public Service)	Identifikovatelné osobní údaje (PII)
	Číslo italského řidičského průkazu	Identifikovatelné osobní údaje (PII)
	Nizozemské číslo BSN (Burgerservicenummer)	Identifikovatelné osobní údaje (PII)
	Norské identifikační číslo	Identifikovatelné osobní údaje (PII)
	Polský identifikační průkaz	Identifikovatelné osobní údaje (PII)
	Polský národní identifikátor (PESEL)	Identifikovatelné osobní údaje (PII)
	Číslo polského pasu	Identifikovatelné osobní údaje (PII)
	Číslo portugalského občanského průkazu	Identifikovatelné osobní údaje (PII)
	Číslo sociálního zabezpečení (SSN) (Španělsko)	Identifikovatelné osobní údaje (PII)
	Národní identifikátor (Švédsko)	Identifikovatelné osobní údaje (PII)
	Číslo pasu (Švédsko)	Identifikovatelné osobní údaje (PII)
	Číslo řidičského průkazu (Spojené království)	Identifikovatelné osobní údaje (PII)
	Voličské číslo (Spojené království)	Identifikovatelné osobní údaje (PII)
	Číslo zdravotního pojištění (Spojené království)	Osobní zdravotní údaje
Číslo národního pojištění (NINO) (Spojené království)	Identifikovatelné osobní údaje (PII)	
Číslo pasu (Spojené státy/Spojené království)	Identifikovatelné osobní údaje (PII)	

Upřesnění výsledků dotazu na typ citlivých informací přidáním parametrů

Do dotazu na typ citlivých informací můžete přidat následující parametry:

- Rozsah počtu – určete, kolik výskytů citlivých informací musí dokument obsahovat, aby byl zahrnut do výsledků dotazu.
- Rozsah pravděpodobnosti – úroveň pravděpodobnosti, že rozpoznání typu citlivých informací skutečně představuje shodu, například 85 (85 %).

K upřesnění dotazů můžete využít také vlastnosti a operátory. Další informace a příklady najdete v článku

[Vytvoření dotazu k vyhledání citlivých dat uložených na webech.](#)

Úprava typu citlivých informací s cílem zvýšit jeho přesnost

Pokud se vám stále nevracejí očekávané výsledky nebo dotaz vrací příliš mnoho falešně pozitivních výsledků, zvažte úpravu typu citlivých informací tak, aby ve vašem prostředí lépe fungoval.

Doporučený postup při vytváření nebo přizpůsobování typu citlivých dat je vytvořit nový typ citlivých dat na základě existujícího typu a dát mu jedinečný název a identifikátory. Pokud například chcete upravit parametry typu citlivých dat Číslo debetní karty EU, můžete svou kopii tohoto pravidla pojmenovat Číslo debetní karty EU – vylepšené a odlišit ji tak od originálu.

`SensitiveType:"<type>|<count range>|<confidence range>"`

`SensitiveType:"Credit Card Number|5"`

(vrátí pouze dokumenty obsahující přesně pět čísel platebních karet)

`SensitiveType:"Credit Card Number|*|85.."`

(rozsah pravděpodobnosti je od 85 % výše)

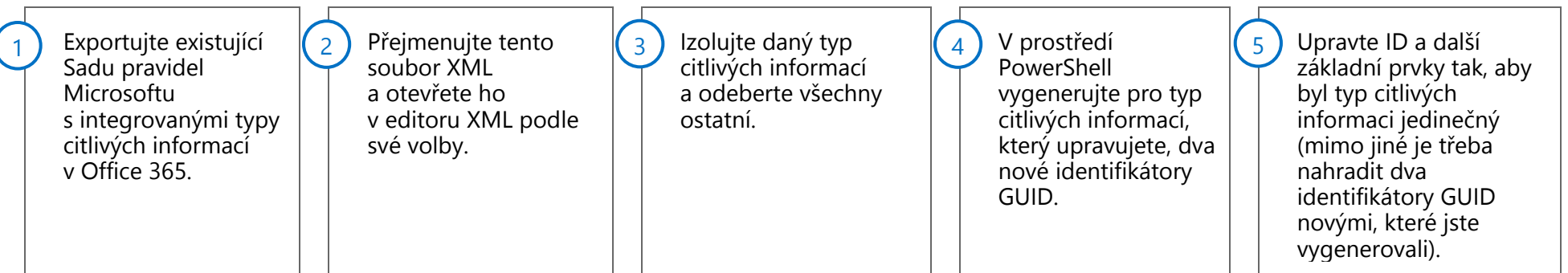
Poznámka: U příkazu SensitiveType se rozlišují velká a malá písmena, u zbytku dotazu však nikoli.

V novém typu citlivých dat jednoduše upravte hodnoty, které chcete změnit, abyste vylepšili jeho přesnost. Jakmile budete hotovi, nahrajete nový typ citlivých dat a vytvoříte nové pravidlo ochrany před únikem informací (případně upravíte stávající pravidlo), které bude právě přidáný nový typ citlivých dat používat. Úprava přesnosti typů citlivých dat může vyžadovat trochu práce metodou pokusu a omylu, je proto dobré uchovat si kopii původního typu, která vám v případě potřeby v budoucnu umožní návrat zpět.

Další informace:

[Přizpůsobení integrovaného typu citlivých informací](#)

[Přizpůsobení nebo vytvoření nového typu citlivých informací pro nařízení GDPR](#), kde najdete podrobný postup <tento článek se připravuje>



6 Zvyšte přesnost vyladěním požadavků na shodu.

Úpravy blízkosti

Upravte blízkost ve vzorci znaků tak, abyste prodloužili nebo zkrátili vzdálenost, ve které se klíčová slova musí nacházet od typu citlivých dat.

Úpravy klíčových slov

Přidejte do jednoho z prvků <Keywords> klíčová slova a poskytněte tak pro typ citlivých dat konkrétnější podpůrné doklady, které se mají vyhledávat jako signál shody s tímto pravidlem. Můžete také odebrat klíčová slova, která vedou k falešně pozitivním výsledkům.

Úpravy pravděpodobnosti

Upravte pravděpodobnost, s kterou musí typ citlivých dat odpovídat kritériím zadaným ve své definici, aby byla signalizována a vykázána shoda.

7 Nový typ citlivých informací nahrajte.

8 Znovu projděte svůj obsah a pokuste se vyhledat citlivé informace.

[Ruční vyžádání prohledání a opětovného indexování webu](#)

Viz také [Přizpůsobení integrovaného typu citlivých informací](#).

Příklad: Úprava typu citlivých informací Číslo debetní karty EU

Zlepšení přesnosti pravidel ochrany před únikem informací v jakémkoli systému vyžaduje testování proti vzorové datové sadě. Může při tom být nutné jemné ladění prostřednictvím opakovaných úprav a testů. V tomto příkladu ukazujeme úpravy typu citlivých informací Číslo debetní karty EU s cílem zlepšit jeho přesnost.

Při hledání čísel debetních karet EU v našem příkladu je definice striktně určuje jako 16 číslic odpovídajících složitému vzorci, které se dají ověřit kontrolním součtem. Vzhledem k definici řetězce tohoto typu citlivých dat nemůžeme tento vzorec změnit. Můžeme ale provést následující úpravy, které zlepšují přesnost při jeho vyhledávání v obsahu v Office 365 s využitím funkce ochrany před únikem informací.

Úpravy blízkosti

Zkrátíme interval úpravou hodnoty `patternProximity` v prvku <Entity> ze 300 na 150 znaků. To znamená, že naše podpůrné doklady (klíčová slova) se k zaznamenání signálu shody s tímto pravidlem musí nacházet blíže k hledanému typu citlivých dat.

```
<Entity id="48da7072-821e-4804-9fab-72ffb48f6f78" patternProximity="150" recommendedConfidence="85">
```

Úpravy klíčových slov

Použití některých klíčových slov může vést k výskytu falešně pozitivních výsledků. Proto může být vhodné klíčová slova odebrat. Tady jsou klíčová slova použita v tomto příkladu:

```
<Keyword id="Keyword_card_terms_dict">
  <Group>
    <Term>corporate card</Term>
    <Term>organization card</Term>
    <Term>acct nbr</Term>
    <Term>acct num</Term>
    <Term>acct no</Term>
    ...
  </Group>
</Keyword>
```

Úpravy pravděpodobnosti

Když odeberete z definice klíčová slova, obvykle budete chtít příslušným snížením této hodnoty zároveň upravit míru svojí jistoty, že byl nalezen daný typ citlivých dat. Výchozí hodnota u typu Číslo debetní karty EU je 85.

```
<Entity id="48da7072-821e-4804-9fab-72ffb48f6f78" patternProximity="150" recommendedConfidence="85">
  <Pattern confidenceLevel="85">
    ...
  </Pattern>
</Entity>
```

Vytváření vlastních dotazů KQL k vyhledání dalších dat ve vašem prostředí

K vyhledání osobních údajů, které podléhají nařízení GDPR, může být nutné vytvořit další dotazy. Ve Vyhledávání obsahu k tomu slouží jazyk KQL (Keyword Query Language). Pokud jej ale použijeme samotný, bez typů citlivých dat, neumožňuje většinu citlivých dat přesně rozpoznat. Cílem tedy je otestovat a optimalizovat řetězce KQL pomocí Vyhledávání obsahu a poté je využít při vytváření a ladění nových typů citlivých dat, s nimiž lze dosáhnout ještě vyšší přesnosti.

K formulování a optimalizaci dotazů v jazyce KQL jsou k dispozici následující zdroje informací:

[Referenční příručka k syntaxi jazyka KQL \(DMC\)](#)

[Spuštění Vyhledávání obsahu v Centru zabezpečení a dodržování předpisů Office 365](#)

Vyhledávání obsahu nabízí další prostředek, který vám s vytvářením dotazů KQL a typů citlivých dat pomůže – klíčová slova. K čemu je seznam klíčových slov užitečný? Můžete získat statistiky, které vám ukážou, kolik položek odpovídá jednotlivým klíčovému slovu. Tak rychle zjistíte, která klíčová slova jsou neefektivnější (a naopak nejméně efektivní). Další informace o statistikách vyhledávání najdete v článku [Zobrazení statistik klíčových slov pro výsledky Vyhledávání obsahu](#).

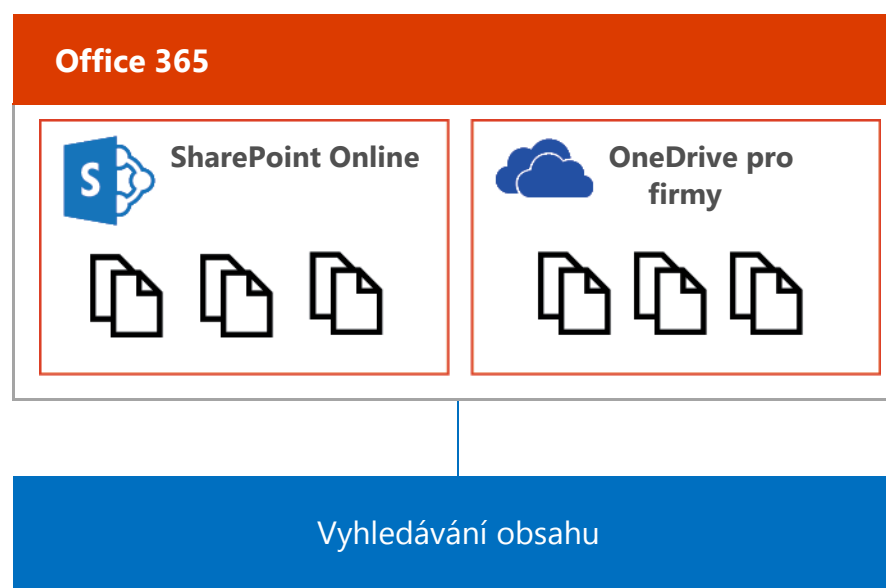
Klíčová slova na jednotlivých řádcích jsou ve vytvořeném vyhledávacím dotazu propojena operátorem NEBO. Na řádku můžete použít také výraz složený z několika klíčových slov (uzavřený v závorkách).

[Dotazy s klíčovými slovy a vyhledávací podmínky ve Vyhledávání obsahu](#)

Příklad – Použití Vyhledávání obsahu k rozpoznání e-mailových adres

E-mailové adresy se pokládají za citlivé informace týkající se subjektů údajů. Tento jednoduchý příklad vám ukáže, jak vám může pomoci Vyhledávání obsahu.

Jazyk KQL a klíčová slova nelze použít současně. Použijte každý z těchto nástrojů samostatně ke zpřesnění dotazu a určení klíčových slov, která mohou být u jednotlivých typů citlivých dat užitečná.



Dotaz KQL

– NEBO –

Klíčová slova

```
(^\\b)([a-zA-Z0-9_\\-\\.]+)@[a-zA-Z0-9_\\-\\.]+\\.([a-zA-Z]{2,5})($\\b)
```

Poznámky:

- Při vyhledávání blízkosti můžete využít operátory NEAR a ONEAR.
- Jazyk KQL bohužel nepodporuje dotazy se třídou regulárního výrazu (např. `IdRef="Regex_email_address"`)

Klíčová slova

e-mailová adresa

mail

kontaktujte

odesílatel

adresát

kopie

skrytá

Tento příklad ukazuje, že klíčová slova nejsou vždy nutná a mohou vést k velkému množství falešně pozitivních výsledků.

Vytváření nových vlastních typů citlivých informací

Poté, co jste použili dotazy KQL a klíčová slova k rozpoznání citlivých informací, můžete na jejich základě vytvořit nové vlastní typy citlivých informací. V mnoha případech budete k dosažení správné míry přesnosti potřebovat propracované typy citlivých informací. Pak můžete tyto vlastní typy citlivých informací použít ve Vyhledávání obsahu, v zásadách ochrany před únikem informací a v rámci dalších dotazů KQL.

Doporučuje se vytvářet nový typ citlivých dat na základě existujícího typu. Postupujte podle kroků, které jsme v tomto tématu již popsali.

Ukážeme si to na příkladu e-mailové adresy, kde je postup dobře vidět.

Příklad úprav nového typu citlivých informací o e-mailu

- 1** Nastavte vlastnost `IdRef`
V rámci prvku `<Entity>` upravte prvek `<IdMatch>` tak, aby se vlastnost `idRef` rovnala jedinečné hodnotě, například `IdRef="Regex_email_address"`. Tato hodnota bude ukazovat na prvek definující náš regulární výraz k vyhledávání e-mailových adres.
`IdRef="Regex_email_address"`
- 2** Atribut blízkosti
V prvku `<Entity>` začneme s hodnotou `patternProximity 300`.
`patternsProximity="300"`
- 3** Úroveň pravděpodobnosti
Vlastnost `recommendedConfidence` nastavte na hodnotu, která podle vašeho názoru vyjadřuje pravděpodobnost nalezení přesné shody. Abyste získali přesný výsledek, budete zřejmě muset hodnotu otestovat s reprezentativní datovou sadou. Jako počáteční nastavení zkuste 75.
`recommendedConfidence="75">`

Prvek entity

Výsledná syntaxe XML po spojení těchto prvních tří prvků vypadá takto:

```
<Entity id="42e6348e-27f0-4774-9604-d470cb3e219a" patternsProximity="300" recommendedConfidence="75">
  <Pattern confidenceLevel="75">
    <IdMatch idRef="Regex_email_address" />
    <Any minMatches="1">
      <Match idRef="Keyword_email_terms" />
    </Any>
  </Pattern>
</Entity>
```

4

Prvek regulárního výrazu

Přidejte bezprostředně pod prvky <Entity> nový prvek <Regex>, který definuje regulární výraz použitý k rozpoznání e-mailových adres. Tento prvek by měl vypadat takto:

```
<Regex id="Regex_email_address">(^|\b)([a-zA-Z0-9_-\.\,]+)@([a-zA-Z0-9_-\.\,]+\.\([a-zA-Z]{2,5}\)\b)</Regex>
```

5

Klíčová slova

Pod prvek <Regex> přidejte nový prvek <Keyword>, který definuje seznam klíčových slov souvisejících s e-mailovými adresami. Zkontrolujte, že hodnota ID prvku <Keyword> odpovídá hodnotě <Match idRef> v prvku <Entity> <Pattern>. Podle potřeby můžete přidávat vlastní klíčová slova.

U tohoto typu citlivých informací pro e-mail nebudou klíčová slova pravděpodobně potřeba. Nabízíme je jen jako příklad.

```
<Keyword id="Keyword_email_terms">
  <Group>
    <Term>email</Term>
    <Term>email address</Term>
    <Term>contact</Term>
  </Group>
</Keyword>
```

6

Prvek LocalizedStrings

V prvku <LocalizedStrings> <Resource> je nutné zadat jedinečný název identifikující typ citlivých dat, například takto:

```
<LocalizedStrings>
  <Resource idRef="42e6348e-27f0-4774-9604-d470cb3e219a">
    <Name default="true" langcode="en-us">Email Address</Name>
    <Description default="true" langcode="en-us">Detects email addresses.</Description>
  </Resource>
</LocalizedStrings>
```

Další příklad použití jazyka KQL a vytvoření vlastního typu citlivých informací

Společnost Contoso používá k identifikaci jednotlivých zákazníků ve své databázi Číslo zákazníka Contoso (CCN). Toto číslo má následující strukturu (tzv. taxonomii):

- Dvě číslice představují rok vytvoření záznamu. Sama společnost Contoso byla založena v roce 2002, nejnižší možná hodnota je tedy 02.
- Tři číslice představují partnerskou agenturu, která záznam vytvořila. Možné hodnoty agentur jsou 000 až 999.
- Písmeno zastupuje linii podnikání. Možné hodnoty jsou a–z, na velikosti při tom nezáleží.
- Čtyřmístné sériové číslo s možnými hodnotami od 0000 do 9999.

Ve společnosti Contoso ve své interní i externí korespondenci, dokumentech atd. vždy na zákazníky odkazují pomocí čísla CCN. Rádi by vytvořili vlastní typ citlivé položky k rozpoznávání použití čísla CCN v Office 365, aby u tohoto typu osobních údajů mohli uplatňovat patřičnou ochranu.

Příklady čísel CCN:

15080P9562
14040O1119
15020J8317
14050E2330
16050E2166
17040O1118

1

Contoso vyhledá dokumenty odpovídající sadě příkladů čísel CCN pomocí prostředí PowerShell a Vyhledávání obsahu.

```
#Připojení k Centru zabezpečení a dodržování předpisů Office 365
$adminUser = "alland@contoso.com"
Connect-IPSSession-UserPrincipalName $adminUser
```

```
#Vytvoření a spuštění vyhledávání ukázkových dat
```

```
$searchName = "Vyhledání ukázkových informací o zákaznících"
$searchQuery = "15080P9562 NEBO 14040O1119 NEBO 15020J8317 NEBO 14050E2330 NEBO 16050E2166 NEBO 17040O1118"
New-ComplianceSearch -Name $searchName -SharePointLocation All -ExchangeLocation All -ContentMatchQuery $searchQuery
Start-ComplianceSearch -Identity $searchName
```

Dotaz KQL

2

Contoso analyzuje získané výsledky.

Při každém použití čísla CCN bylo zároveň použito datum ve formátu EU a také jedno z následujících klíčových slov v blízkosti do 300 znaků:

číslo zákazníka, zákaznické číslo, č. zákazníka, zákazník čís., zákazník Contoso

3

K rozpoznání čísel CCN vytvořili ve společnosti Contoso následující regulární výraz (RegEx).

```
[0-1][0-9][0-9]{3}[A-Za-z][0-9]{4}
```

4

K rozpoznání dat EU ve formátech používaných různými pobočkami vytvořili ve společnosti Contoso následující regulární výraz (RegEx).

```
(0?[1-9]|[12][0-9]|3[0-1])[V-](0?[1-9]|1[0-2])j|x00e4n(uar)?jan(uary|uari|uar|eiro|vier|v)?|ene(ro)?|genn(aio)?|feb(ruary|ruari|rero|braio|ruar|br)?|f\x00e9vr(ier)?|fev(ereiro)?|mar(zo|o|ch|s)?|m\x00e4rz|maart|apr(ile|il)?|abr(il)?|avril|may(o)?|magg(io)?|mai|mei|mai(o)?|jun(io|i|e|ho)?|giugno|juin|jul(y|io|i|ho)?|lu(glio)?|juil(let)?|ag(o|osto)?|aug(ustus|ust)?|ao\x00fbt|sep|sept(ember|iembre|embre)?|sett(embre)?|set(embro)?|oct(ober|ubre|obre)?|ott(obre)?|okt(ober)?|out(ubro)?|nov(ember|iembre|embre|embro)?|dec(ember)?|dic(iembre|embre)?|dez(ember|embro)?|d\x00e9c(embre)?[V-](19|20)?[0-9]{2}
```

5 V prostředí PowerShell ve společnosti Contoso vygenerují tři jedinečné identifikátory GUID.

```
#Vygenerování jedinečného identifikátoru GUID pro ID balíčku pravidel, vydavatele a prvku  
[guid]::NewGuid().Guid  
[guid]::NewGuid().Guid  
[guid]::NewGuid().Guid
```

6 Contoso definuje pro pravidlo vlastního typu citlivé položky následující parametry:

Název: Číslo zákazníka Contoso (CCN)

Popis: Číslo zákazníka Contoso (CCN), s kterým se zároveň vyhledávají další klíčová slova a datum ve formátu EU

8 Contoso vytvoří pro nový typ citlivé informace k rozpoznání čísla zákazníka Contoso (CCN) soubor XML a uloží jej do místního souborového systému C:\Scripts\ContosoCCN.xml se šifrováním UTF-8.

```
<?xml version="1.0" encoding="utf-8"?>  
<RulePackage xmlns="http://schemas.microsoft.com/office/2011/mce">  
<RulePack id="130ae63b-a91e-4a12-9e02-a90e36a83d7f">  
<Version major="1" minor="0" build="0" revision="0" />  
<Publisher id="47148982-defd-42a1-890a-7b9472099f1f" />  
<Details defaultLangCode="en">  
<LocalizedDetails langcode="en">  
<PublisherName>Contoso Ltd.</PublisherName>  
<Name>Contoso Rule Package</Name>  
<Description>Defines Contoso's custom set of classification rules</Description>  
</LocalizedDetails>  
</Details>  
</RulePack>  
<Rules>  
<!-- Contoso Customer Number (CCN) -->  
<Entity id="a91f9a2e-6cfc-4622-8c5d-954875aa5b2b" patternsProximity="300"  
recommendedConfidence="85">  
<Pattern confidenceLevel="85">  
<IdMatch idRef="Regex_contoso_ccn" />  
<Match idRef="Keyword_contoso_ccn" />  
<Match idRef="Regex_eu_date" />  
</Pattern>  
</Entity>  
<Regex id="Regex_contoso_ccn">[0-1][0-9][0-9]{3}[A-Za-z][0-9]{4}</Regex>  
<Keyword id="Keyword_contoso_ccn">  
<Group matchStyle="word">  
<Term caseSensitive="false">customer number</Term>  
<Term caseSensitive="false">customer no</Term>  
<Term caseSensitive="false">customer #</Term>  
<Term caseSensitive="false">customer#</Term>  
<Term caseSensitive="false">Contoso customer</Term>  
</Group>  
</Keyword>  
<Regex id="Regex_eu_date"> (0?[1-9]|[12][0-9]|3[0-1])[V-](0?[1-9]|1[0-2])j\  
x00e4n(uar)?jan(uary|uari|uar|eiu|vier|v)?ene(ro)?genn(aio)? |feb(ruary|ruari|rero|braio|ruar|br)?f\  
x00e9vr(ier)?fev(ereiro)?mar(zo|o|ch|s)?m\x00e4rz|maart|apr(ile|il)?abr(il)?avril\  
|may(o)?magg(io)?mai|mei|mai(o)?jun(io|i|e|ho)?giugno|juin|jul(y|io|i|ho)?lu(glio)?juil(let)?ag(o|  
osto)?aug(ustus|ust)?ao\  
x00fbt|sep|sept(ember|iembre|embre)?sett(embre)?set(embro)?oct(ober|ubre|obre)?ott(obre)?o  
kt(ober)?out(ubro)?  
|nov(ember|iembre|embre|embro)?dec(ember)?dic(iembre|embre)?dez(ember|embro)?d\  
x00e9c(embre)?[ V-](19|20)?[0-9]{2}</Regex>  
<LocalizedStrings>  
<Resource idRef="a91f9a2e-6cfc-4622-8c5d-954875aa5b2b">  
<Name default="true" langcode="en-us">Contoso Customer Number (CCN)</Name>  
<Description default="true" langcode="en-us">Contoso Customer Number (CCN) that looks for  
additional keywords and EU formatted date</Description>  
</Resource>  
</LocalizedStrings>  
</Rules>  
</RulePackage>
```

Zkontrolujte, že šifrování zadané na tomto místě odpovídá šifrování uloženého souboru.

GUID balíčku pravidel z kroku 5

GUID vydavatele z kroku 5

GUID entity z kroku 5

Shoda ID

Regulární výraz pro číslo CCN z kroku 3

Shoda ID

Regulární výraz pro datum EU z kroku 4

GUID entity z kroku 5

Název z kroku 6

Popis z kroku 6

9 Contoso vytvoří vlastní typ citlivých informací následujícím příkazem PowerShell:

```
#Připojení k Centru zabezpečení a dodržování předpisů Office 365  
$adminUser = "alland@contoso.com"  
Connect-IPPSSession -UserPrincipalName $adminUser  
  
#Vytvoření nového typu citlivých informací  
New-DlpSensitiveInformationTypeRulePackage -FileData C:\Scripts\ContosoCCN.xml
```

Architektura schématu kategorizace osobních údajů

Do tohoto okamžiku jsme se soustředili na využití typů citlivých informací k rozpoznání osobních údajů podléhajících nařízení GDPR. Typy citlivých informací představují formu kategorizace a mohou být jedinou kategorizací, kterou budete potřebovat. Mnoho organizací však zavádí širší strategii řízení dat s využitím popisků. Toto téma vám pomůže posoudit, zda je pro vás užitečné v rámci plánu GDPR popisky implementovat. Pokud se k tomu rozhodnete, nabízíme v tomto tématu užitečné rady a příklady.

Poznámka: Stanovení kategorizačního schématu organizace a konfigurace zásad, popisků a podmínek vyžaduje pečlivé plánování a přípravu. Je důležité si uvědomit, že tento proces není řízen oddělením IT. Při vytváření vhodného schématu kategorizace a popisků dat používaných ve vaší organizaci je zcela zásadní spolupráce právního oddělení a týmu pro soulad s předpisy.

Rozhodnutí, zda budete vedle typů citlivých informací používat také popisky

Při kategorizaci osobních údajů v Office 365 můžete volit mezi dvěma přístupy. Pro ochranu údajů v souladu s nařízením GDPR lze použít kterýkoli z nich.

Pokud ke kategorizaci využíváte pouze typy citlivých informací, můžete zbytek tohoto tématu přeskocit.

Použití samotných typů citlivých informací v Office 365

- Typy citlivých informací umožňují dobře rozpoznat a chránit osobní údaje podléhající nařízení GDPR a dalším typům regulací.
- Pokud vaše organizace dosud nemá širší plán řízení dat ani se jej nechystá zavést, je použití typů citlivých informací jednodušší.
- Fungují v kombinaci s pravidly ochrany před únikem informací (podobně jako popisky Office).
- V budoucnu je bude možné použít spolu se službou Cloud App Security k rozpoznání citlivých informací v dalších aplikacích SaaS.

– NEBO –

Použití typů citlivých informací a popisků Office

- Typy citlivých informací budete potřebovat k automatickému přiřazení popisků k osobním údajům podléhajícím nařízení GDPR, jejich použití je tedy nezbytné.
- Použití popisků Office dovoluje zahrnout osobní údaje podléhající nařízení GDPR do širšího plánu řízení dat ve vaší organizaci.
- Časem se popisky Office sjednotí s popisky služby Azure Information Protection do jednoho kategorizačního modulu.

Vytvoření schématu popisků zahrnujícího osobní údaje

Než začnete uplatňovat technické možnosti zavádění popisků a ochrany, nejprve v rámci organizace definujte kategorizační schéma. Je možné, že vaše organizace už podobné schéma používá, takže ho bude třeba jen doplnit o osobní údaje. Toto téma obsahuje příklad kategorizačního schématu, který můžete v případě potřeby využít jako odrazový bod.

Jak začít

Začněte určením počtu popisků, které chcete zavést, a jejich názvů. Nezapomínejte se při tom tím, jakou technologii použijete a jak se popisky uplatní. Toto schéma je vhodné použít univerzálně v celé organizaci, včetně dat uložených místně nebo v jiných cloudových službách.

Doporučení

Při návrhu a implementaci zásad, popisků a podmínek vezměte v potaz následující doporučení:

- **Pokud můžete, použijte stávající kategorizační schéma** – Mnoho organizací již kategorizaci dat v nějaké podobě využívá. Pečlivě zhodnotte stávající schéma popisků a pokud je to možné, použijte ho tak, jak je. Známé, rozpoznatelné popisky zvyšují přijetí tohoto prvku mezi koncovými uživateli.
- **Začněte výchozími zásadami a popisky** – Všechna řešení obsahují sadu předdefinovaných zásad a popisků. Pečlivě je posuďte s ohledem na právní a obchodní požadavky organizace a zvažte, zda je možné je použít a nevytvářet nové.
- **Začněte v malém** – Pro počet vytvořených popisků prakticky neexistuje omezení. Velké množství popisků a dílčích popisků ale negativně ovlivňuje přijetí mezi uživateli. Při nadměrném velkém výběru je pro uživatele často nejjednodušší nevybírat nic.
- **Využijte scénáře a případy použití** – Určete v organizaci běžné případy použití a pomocí scénářů odvozených z nařízení GDPR ověřte, zda bude zamýšlená konfigurace popisků a kategorizace fungovat v praxi.

Příklad kategorizačního schématu

Název popisku	Popis
Osobní	Data, která nejsou obchodní, určená pouze pro osobní použití
Veřejné	Obchodní data zvláště připravená a schválená pro veřejné použití
Údaje o zákaznících	Obchodní data obsahující identifikovatelné osobní údaje. Příkladem jsou čísla platebních karet, bankovních účtů nebo zdravotní pojištění.
Personální údaje	Data personálního oddělení o zaměstnancích společnosti Contoso, jako jsou osobní čísla a údaje o mzdách
Důvěrné	Citlivá obchodní data, jejichž sdílení s neoprávněnými osobami by mohlo poškodit podnik. Patří k nim smlouvy, zprávy o zabezpečení, souhrny prognóz a údaje o prodeji.
Vysoce důvěrné	Velmi citlivá obchodní data, jejichž sdílení s neoprávněnými osobami by mohlo poškodit podnik. Patří k nim údaje o zaměstnancích a zákaznících, hesla, zdrojový kód nebo předběžně ohlášené finanční zprávy.

- **Zvažte každý požadavek na nový popisek** – Opravdu každý scénář či případ použití potřebuje nový popisek, nebo můžete využít některý z těch stávajících? Udržení množství popisků na minimu zvyšuje přijetí mezi uživateli.
- **Použijte dílčí popisky pro klíčová oddělení** – Některá oddělení budou mít zvláštní potřeby vyžadující specifické popisky. Definujte tyto popisky jako dílčí k existujícímu popisku a zvažte použití zásad s rozsahem, které se nepřizpůsobují globálně, ale konkrétním skupinám uživatelů.
- **Zvažte použití zásad s rozsahem** – Tyto zásady cílené na dílčí sady uživatelů pomohou předejít „zahlcení popisky“. Zásady s rozsahem umožňují přiřazovat popisky (nebo dílčí popisky) specifické pro konkrétní roli či oddělení pouze těm zaměstnancům, kteří v daném oddělení pracují.
- **Používejte vypovídající názvy popisků** – Doporučuje se nepoužívat v názvech popisků žargon, názvy norem ani jiné zkratky. Snažte se podpořit přijetí mezi koncovými uživateli volbou názvů, které jim budou srozumitelné. Místo popisků typu PII, PCI, HIPAA, LBI, MBI nebo HBI zvažte názvy jako Nefiremní, Veřejné, Obecné, Důvěrné a Vysoce důvěrné.

Určení taxonomie a vyhledávacích kritérií každého popisku

Dalším krokem po vytvoření kategorizačního schématu organizace je určení taxonomie a kritérií pro vyhledávání těchto dat. U osobních údajů jste již tento krok provedli, když jste určili typy citlivých informací a případně si je přizpůsobili pro své prostředí nebo vytvořili nové.

Následující tabulka obsahuje příklad schématu, taxonomie a vyhledávacích kritérií v organizaci. Popisky jsou uspořádány podle úrovně citlivosti od nejméně citlivé po nejcitlivější, aby bylo zajištěno přiřazení odpovídajícího popisku u dat, jež vyhovují podmínkám několika popisků.

Poznámka: Příklad konfigurace je pouze ilustrační a nemá sloužit jako pokyn ani referenční informace k nasazení.

Důležité je zajistit, aby výsledky práce, kterou investujete do kategorizace osobních údajů pro účely shody s nařízením GDPR, odpovídaly cílům celé vaší organizace.

Příklad schématu, taxonomie a vyhledávacích kritérií

Popisky	Taxonomie	Metoda	Vyhledávací syntaxe
Osobní	Dokumenty ručně označené koncovým uživatelem jako osobní	Ručně	Dokumenty ručně označené koncovým uživatelem jako osobní
Veřejné	Dokumenty obsahující výraz (bez rozlišení velkých a malých písmen) Schváleno ke zveřejnění ##/#### , kde znak # zastupuje jakoukoli číslici	KQL	Schváleno ke zveřejnění*
		RegEx	(?i)(\bApproved for Public Release\d{2}\d{4}\b)
Údaje o zákaznících	Typy citlivých informací v údajích o občanech EU Vlastní typy citlivých informací pro další identifikovatelné osobní údaje	Typy citlivých informací	
Personální oddělení – údaje o zaměstnancích	Dokumenty obsahující ID zaměstnance (s rozlišením velikosti písmen) ve formátu CONTOSO-9##### , kde znak # zastupuje libovolnou číslici	KQL	CONTOSO-9*
		RegEx	(\bCONTOSO-9\d{5}\b)
Personální oddělení – údaje o mzdách	Dokumenty obsahující klíčové slovo (bez rozlišení velkých a malých písmen) Contoso A kterékoli z klíčových slov (bez rozlišení velkých a malých písmen) mzda NEBO odměna	KQL	Contoso A (mzda NEBO odměna)
		RegEx	(\bCONTOSO-9\d{5}\b)
Důvěrné	Dokumenty obsahující výraz (bez rozlišení velkých a malých písmen) Contoso – důvěrné	KQL	Contoso – důvěrné
		RegEx	(?i)(\bContoso Confidential\b)
Vysoce důvěrné	Dokumenty obsahující některý z výrazů (s rozlišením velkých a malých písmen) Contoso – tajné nebo Tajné-C#### , kde znak # zastupuje libovolnou číslici	KQL	Contoso – tajné NEBO Tajné-C*
		RegEx	(?i)(\bContoso Secret\b)(\bSecret-C\d{4}\b)

Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

Toto je 4. téma ze sedmidílné série.



Použití popisků u osobních údajů v Office 365

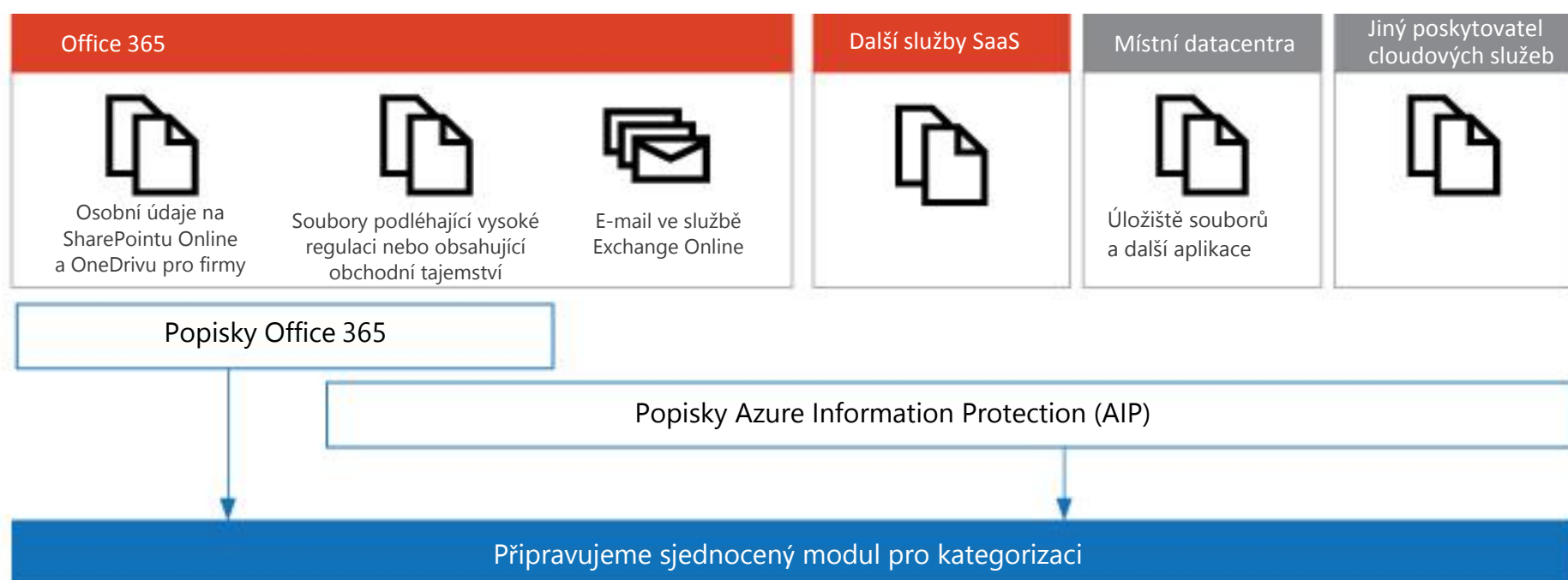
V tomto tématu najdete užitečné informace, pokud v rámci plánu ochrany údajů podle nařízení GDPR používáte popisky Office. Momentálně lze popisky vytvářet v Centru zabezpečení a dodržování předpisů Office 365 a ve službě Azure Information Protection. Později budou tyto technologie sloučeny do jednotného modulu pro popisky a kategorizaci, který nabídne ještě více funkcí.

Používáte-li na ochranu osobních údajů v Office 365 popisky, doporučuje Microsoft začít popisky Office. Ve službě Advanced Data Governance můžete popisky automaticky přiřadit na základě typů citlivých informací nebo jiných kritérií. Popisky Office v kombinaci s ochranou před únikem informací vám zajistí zabezpečení. Můžete je použít také společně s funkcí eDiscovery a Vyhledáváním obsahu. Zanedlouho budete moci popisky i typy citlivých informací používat se službou Cloud App Security k monitorování osobních údajů uložených v dalších aplikacích SaaS.

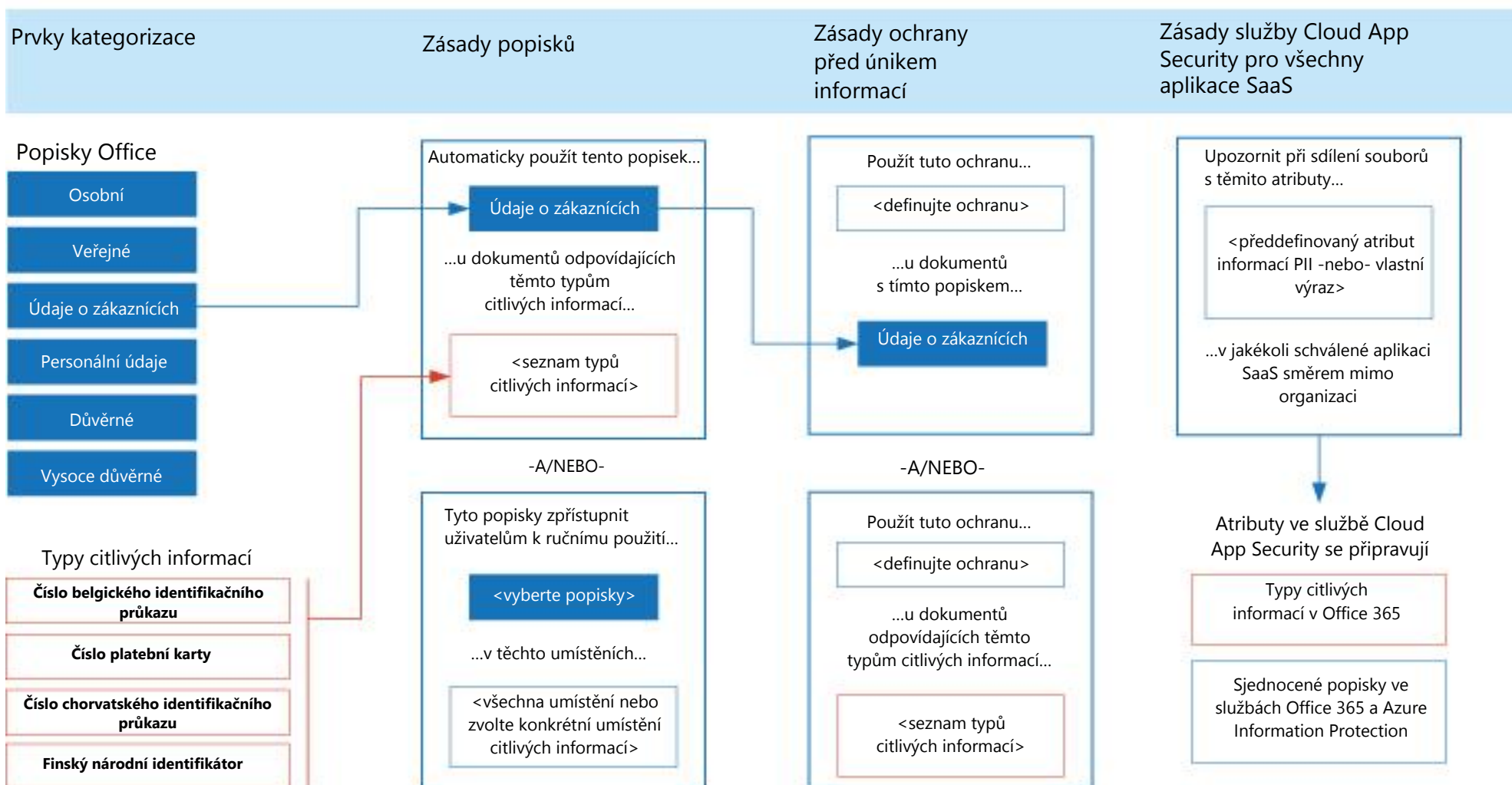
Popisky služby Azure Information Protection momentálně doporučujeme použít při přiřazování popisků místním souborům a souborům v dalších cloudových službách nebo u jiných poskytovatelů. Doporučují se také pro soubory v Office 365, u nichž ochrana dat vyžaduje šifrování Azure Rights Management (Azure RMS), například pro soubory obsahující obchodní tajemství.

Pro soubory Office 365 obsahující data, která podléhají nařízení GDPR, se použití služby Azure Information Protection k uplatnění šifrování Azure RMS v současné době nedoporučuje. Služby Office 365 aktuálně nedokážou soubory se šifrováním RMS číst, takže v nich nenaleznou citlivá data.

Popisky Azure Information Protection lze použít u pošty ve službě Exchange Online a fungují společně s ochranou před únikem informací v Office 365. Zanedlouho zpřístupníme jednotný modul pro kategorizaci a popisky, který umožní používat stejné popisky u e-mailů a souborů a nabídne automatické přiřazování popisků a ochranu pošty během přenosů.



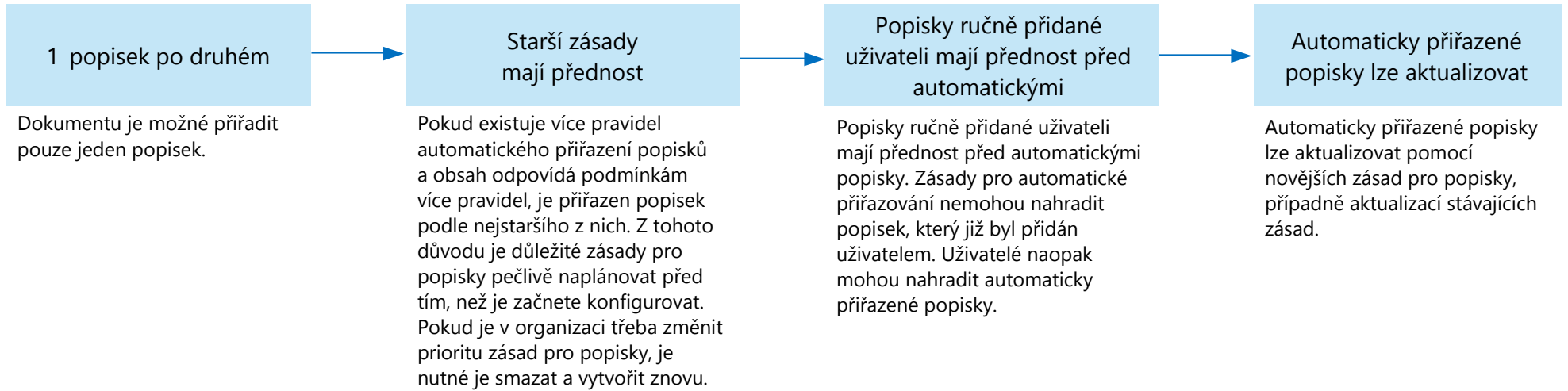
Použití popisků Office a typů citlivých informací ve službách Microsoft 365 k ochraně informací



Priorita pro zásady automatického používání popisků

U osobních údajů podléhajících nařízení GDPR doporučuje společnost Microsoft automatické používání popisků s využitím typů citlivých informací, které jste ve vašem prostředí určili. Zásady automatického uplatňování popisků je důležité kvalitně navrhnout a otestovat, zda se chovají tak, jak jste zamýšleli.

Na výsledek má vliv pořadí, ve kterém byly zásady automatického používání vytvořeny, a také skutečnost, zda popisky zároveň uplatňují také uživatelé. Zavedení zásad je tedy nutné pečlivě naplánovat. V úvahu je při tom třeba vzít následující skutečnosti.



Do plánu pro implementaci popisků nezapomeňte zahrnout:

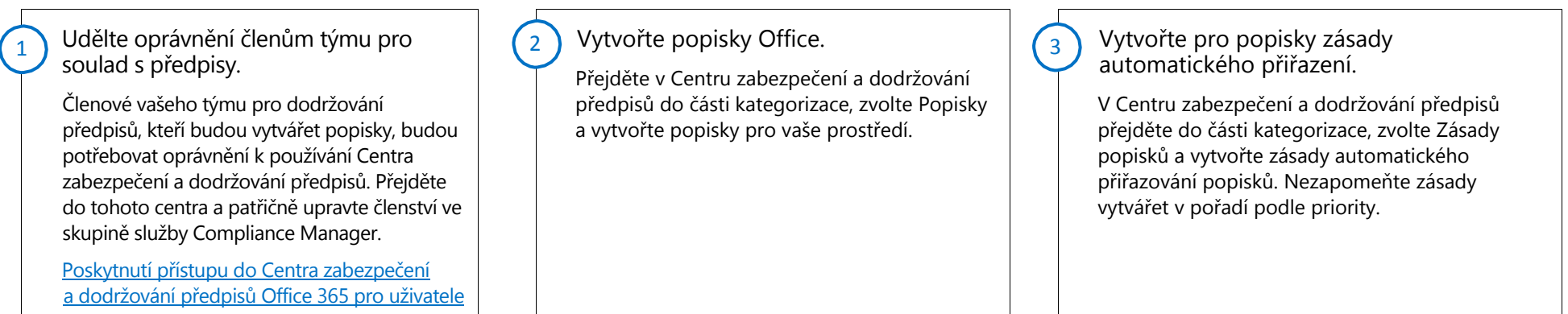
- Prioritu pořadí, ve kterém jsou zásady pro automatické používání vytvořeny.
- Dostatek času pro automatické přiřazení popisků před tím, než je uvolníte uživatelům k ručnímu přidávání. Přiřazení popisků k veškerému obsahu, který odpovídá podmínkám, může trvat až sedm dní.

Příklad priority při vytváření zásad pro automatické používání popisků

Popisky	Pořadí priority při vytváření zásad pro automatické používání
Personální oddělení – údaje o zaměstnancích	1
Údaje o zákaznících	2
Vysoce důvěrné	3
Personální oddělení – údaje o mzdách	4
Důvěrné	5
Veřejné	6
Osobní	Žádné zásady automatického použití

Vytváření popisků a zásad jejich automatického používání

Popisky a zásady se vytvářejí v Centru zabezpečení a dodržování předpisů

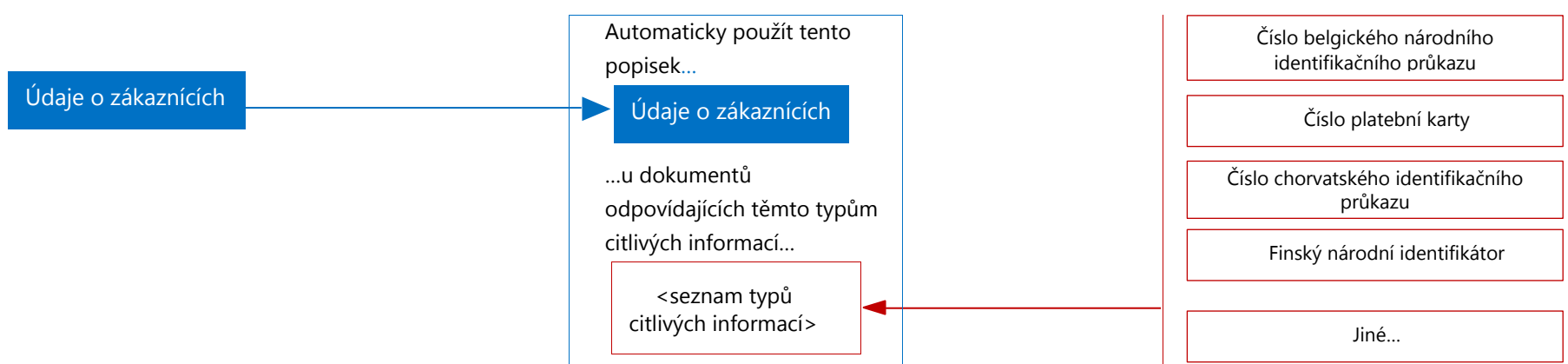


Popisky osobních údajů o zákaznících s ohledem na nařízení GDPR

Vytvořte popisek pro údaje o zákaznících.

Vytvořte zásadu automatického použití, která přiřadí popisek „Údaje o zákaznících“ všem souborům obsahujícím tento typ citlivých informací.

Přidejte všechny typy citlivých informací, které jste vytvořili pro vaše prostředí pro účely souladu s nařízením GDPR.



Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

Toto je 5. téma ze sedmidílné série.



Použití ochrany u citlivých dat v Office 365

Ochrana osobních údajů v Office 365 zahrnuje funkce ochrany před únikem informací. Pomocí zásad ochrany před únikem informací (DLP) v Centru zabezpečení a dodržování předpisů Office 365 můžete rozpoznávat, monitorovat a automaticky chránit citlivé informace ve všech službách Office 365.

Toto téma popisuje použití ochrany před únikem informací k ochraně osobních údajů. Zároveň shrnuje další ochranné funkce, které lze využít při zajišťování shody s nařízením GDPR, včetně nastavení oprávnění v knihovně SharePointu nebo zásad pro přístup k zařízením.

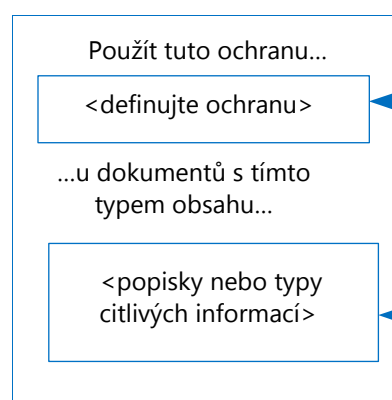
Použití ochrany před únikem informací k ochraně dat v Office 365

S funkcí ochrany před únikem informací můžete:

- Rozpoznat citlivé informace v mnoha různých umístěních
- Předejít nechtěnému sdílení citlivých informací
- Pomoci uživatelům v dodržení předpisů, aniž by to narušilo chod jejich práce
- Zobrazit sestavy DLP s obsahem odpovídajícím zásadám ochrany před únikem informací ve vaší organizaci

[Další informace najdete v článku Přehled zásad ochrany před únikem informací.](#)

Zásady ochrany před únikem informací



Ochrana může zahrnovat:

- Typy k zásadám pro uživatele
- E-mailový přehled pro správce
- Zákaz externího, interního nebo veškerého sdílení

Spolu se zásadami ochrany před únikem informací můžete použít typy citlivých informací nebo popisky

Použití ochrany před únikem informací k zajištění shody s nařízením GDPR

Jedním z primárních využití ochrany před únikem informací v Office 365 je rozpoznat ve vašem prostředí Office 365 osobní údaje týkající se subjektů údajů v EU. Pomocí ochrany před únikem informací v Office 365 mohou vaše týmy pro soulad s předpisy získat upozornění, kde jsou na SharePointu Online a OneDrivu pro firmy uloženy osobní údaje nebo kdy uživatelé odesílají e-maily obsahující osobní údaje. Ochrana před únikem informací může také poskytovat upozornění na možný únik citlivých informací vašim zaměstnancům, kteří pracují s osobními údaji rezidentů Evropské unie.

Jednou z úrovní ochrany informací pomocí funkce DLP v Office 365 je i zvyšování povědomí zaměstnanců o tom, kde jsou ve vašem prostředí uloženy údaje rezidentů EU a jak mají zaměstnanci povoleno s nimi nakládat. Zaměstnanci, kteří již mají k údajům tohoto typu přístup, jej často potřebují ke své každodenní práci. Prosazování zásad ochrany před únikem informací s cílem zajistit soulad s nařízením GDPR nemusí nutně vyžadovat omezování přístupu.

Příklady úrovní ochrany, které lze nakonfigurovat pomocí zásad ochrany před únikem informací a použít k zajištění shody s nařízením GDPR

Úroveň ochrany	Konfigurace DLP pro dokumenty s osobními údaji, které se týkají subjektů údajů v EU	Přínosy a rizika
Informovanost	<ul style="list-style-type: none">• Odesílání e-mailových oznámení týmům pro dodržování předpisů, když jsou v dokumentech na SharePointu Online a OneDrivu pro firmy nalezeny osobní údaje• Přizpůsobení a zobrazení upozornění na možný únik osobních údajů, když zaměstnanci otevírají na SharePointu Online a OneDrivu pro firmy dokumenty obsahující tyto údaje• Rozpoznání sdílení těchto údajů a jeho ohlášení	<ul style="list-style-type: none">• Zvyšování povědomí o místech uložení osobních údajů v týmech pro dodržování předpisů a mezi zaměstnanci• Informování zaměstnanců o firemních zásadách pro zacházení s dokumenty obsahujícími osobní údaje• Nebrání zaměstnancům v interním ani externím sdílení těchto údajů.• Na základě sestav DLP se sdílenými daty můžete rozhodnout o posílení ochrany.
Prevence externího sdílení	<ul style="list-style-type: none">• Omezení přístupu k dokumentům na SharePointu Online a OneDrivu pro firmy, které obsahují osobní údaje, pokud je obsah sdílen s externími uživateli• Zabránění v odesílání e-mailů s dokumenty, které obsahují osobní údaje, externím příjemcům• Rozpoznání sdílení těchto údajů a jeho ohlášení.	<ul style="list-style-type: none">• Zabránění externímu sdílení těchto údajů, ale umožňuje zaměstnancům pracovat s nimi interně.• Na základě sestav DLP s interně sdílenými daty můžete rozhodnout o posílení ochrany.
Prevence interního a externího sdílení	<ul style="list-style-type: none">• Omezení přístupu k dokumentům obsahujícím osobní údaje na OneDrivu pro firmy a SharePointu Online, pokud je obsah sdílen s interními nebo externími uživateli• Zabránění v odesílání e-mailů, které obsahují osobní údaje, interním i externím příjemcům	<ul style="list-style-type: none">• Zabránění internímu a externímu sdílení osobních údajů.• Zaměstnanci možná nebudou moci provádět úkoly vyžadující práci s těmito údaji.• Na základě sestav DLP s interně nebo externě sdílenými daty můžete rozhodnout, zda je nutné školení koncových uživatelů.

Poznámka: Zvyšující se úroveň ochrany v některých případech omezuje možnosti zaměstnanců co do přístupu k informacím, což potenciálně může snižovat jejich produktivitu nebo schopnost plnit každodenní úkoly.

Zvýšení úrovně ochrany zavedením zásad, jež mají dopad na zaměstnance, obvykle doprovází školení koncových uživatelů a informování uživatelů o nových zásadách a postupech zabezpečení. Cílem je umožnit jim dále produktivně pracovat v bezpečnějším prostředí.

Příklad zásady DLP pro úroveň GDPR – Informovanost

Název: Informovanost o osobních údajích podléhajících nařízení GDPR	
Popis: Zobrazení upozornění na možný únik citlivých informací pro zaměstnance, oznámení týmům pro dodržování předpisů, když jsou v dokumentech na SharePointu Online a OneDrivu pro firmy nalezeny osobní údaje, rozpoznání sdílení těchto údajů mimo organizaci a jeho ohlášení	
Ovládací prvek	Nastavení
Určit informace, které mají být chráněny	Vyberte šablonu zásady Vlastní.
Umístění	Všechna umístění v Office 365
Najít obsah, který obsahuje	Klikněte na Upravit a přidejte všechny typy citlivých informací, které jste vytvořili pro vaše prostředí.
Zjišťovat sdílení tohoto obsahu	Zaškrtněte toto políčko a vyberte možnost „s lidmi mimo naši organizaci“.
Upozornit uživatele, pokud obsah odpovídá nastavení zásad	Zaškrtněte toto políčko („Umožňuje zobrazit uživatelům upozornění na možný únik citlivých informací a poslat jim oznámení e-mailem“). Klikněte na možnost Přizpůsobit upozornění a e-mail a aktualizujte text pro vaše prostředí. Výchozí upozornění najdete v tomto článku: Odesílání e-mailových oznámení a zasílání upozornění na možný únik citlivých informací podle zásad DLP.
Zjišťovat sdílení určitého množství citlivých informací najednou	<ul style="list-style-type: none"> „Zjišťovat sdílení dat, která obsahují: Nejméně ____ instance/instancí citlivých informací stejného typu“ – Nastavte tuto volbu na 1. „Posílat hlášení incidentů e-mailem“ – toto políčko zaškrtněte. Klikněte na Zvolte, co chcete zahrnout do hlášení a kdo ho bude dostávat. Nezapomeňte mezi adresáty přidat tým pro dodržování předpisů. Omezit, kdo může získat přístup k obsahu a přepsat zásady – zrušte zaškrtnutí tohoto políčka, abyste dostávali upozornění o citlivých informacích a nebránili přitom uživatelům v přístupu k nim.

Všechna umístění zahrnují:

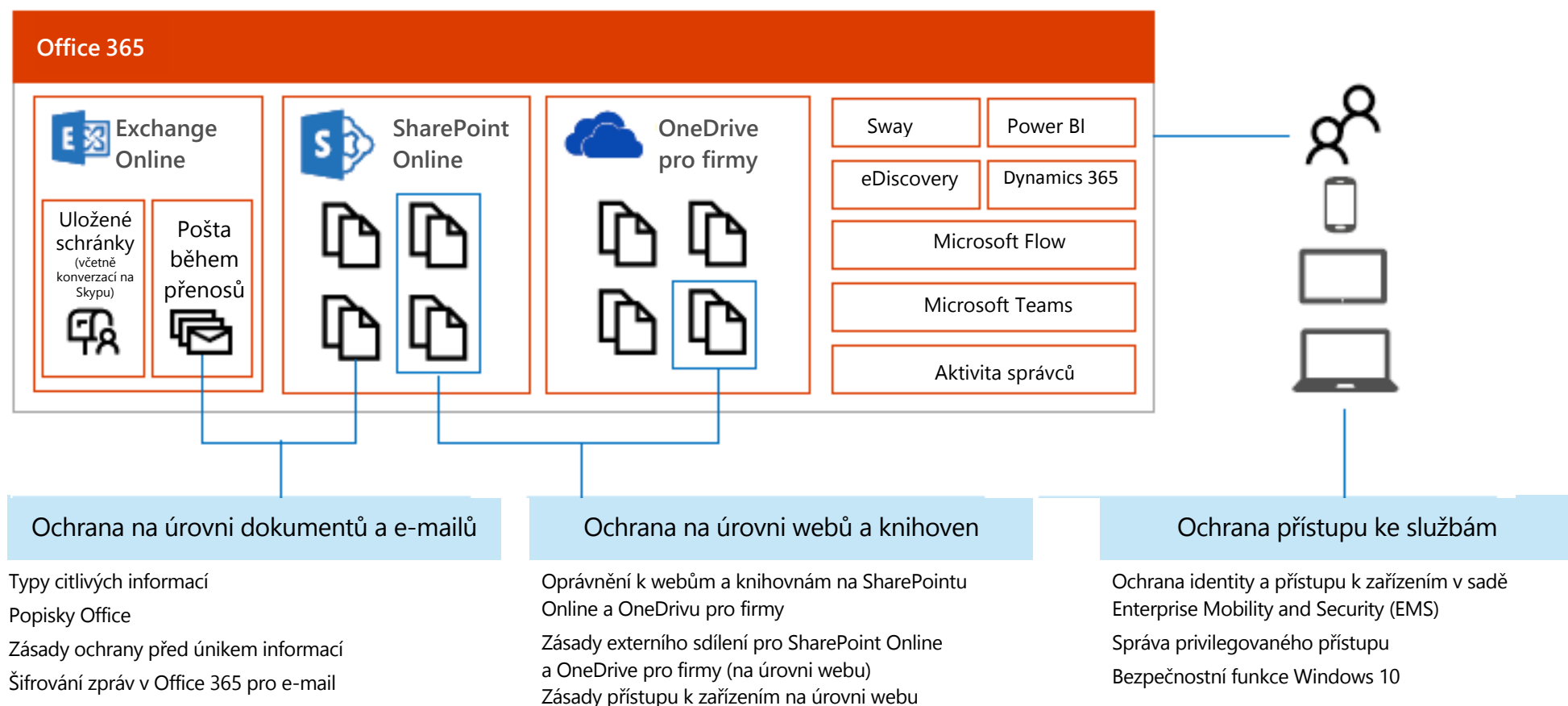
- SharePoint Online
- Účty OneDrivu pro firmy
- Poštovní schránky Exchange

Protože Vyhledávání obsahu aktuálně neumožňuje testovat typy citlivých informací s e-maily, může být užitečné vytvořit pro Exchange samostatné zásady s dílčí sadou typů citlivých informací v každé z nich a poté monitorovat jejich zavedení.

Další typy ochrany, které můžete uplatnit u osobních údajů v Office 365

Typy citlivých informací, popisky a zásady ochrany před únikem informací pomáhají při rozpoznávání dokumentů obsahujících konkrétní data a při použití ochrany. Tyto možnosti ochrany však závisí na vhodném nastavení oprávnění pro přístup k datům, na tom, aby účty uživatelů nebyly narušeny a zařízení byla v dobrém stavu.

Následující schéma ilustruje další typy ochrany, které můžete u osobních údajů uplatnit.



Funkce, které lze používat s nařízením GDPR

V prostředí konfigurovaném s ohledem na soulad s nařízením GDPR lze používat následující funkce. Tyto funkce nejsou nezbytné pro dodržení nařízení GDPR, ale je možné je používat, aniž by to mělo negativní vliv na vyhledávání, ochranu, monitorování a ohlašování údajů, jež s dodržением nařízení GDPR souvisejí.

Klíč zákazníka – Umožňuje zákazníkům poskytovat a zachovat si kontrolu nad šifrovacími klíči používanými k šifrování dat uložených v Office 365. Doporučuje se pouze zákazníkům, od nichž regulace vyžaduje, aby své šifrovací klíče spravovali sami.

Customer Lockbox – Tato služba vám umožňuje ponechat si kontrolu nad přístupem technika Microsoftu k vašim datům, pokud je to třeba k vyřešení technického problému, a to na bázi jednotlivých případů. Vždy můžete rozhodnout, zda technikovi přístup k datům poskytnete, nebo ne. Každý požadavek má omezenou platnost.

Ochrana na úrovni webů a knihoven

Oprávnění ke knihovnám SharePointu a OneDrivu pro firmy

Oprávnění na SharePointu můžete využít k poskytnutí nebo omezení přístupu k webu nebo k jeho obsahu. Můžete do výchozích skupin na SharePointu přidávat jednotlivé uživatele nebo skupiny Azure Active Directory, případně si vytvořit vlastní skupinu, nad níž máte podrobnější kontrolu.

Další informace:

[Principy úrovní oprávnění na SharePointu](#)

[Principy skupin SharePointu](#)



Úplné řízení zobrazení	Návrh	Úpravy	Přispívání	Čtení	Pouze
	Přispívání + schvalování a úpravy	Přispívání + přidávání, úpravy a odstraňování seznamů (ne pouze jejich položek)	Zobrazení, přidávání, aktualizace a odstraňování položek seznamů a dokumentů	Zobrazení a stahování	Zobrazení, bez stahování

Zásady externího sdílení pro knihovny SharePointu a OneDrivu pro firmy

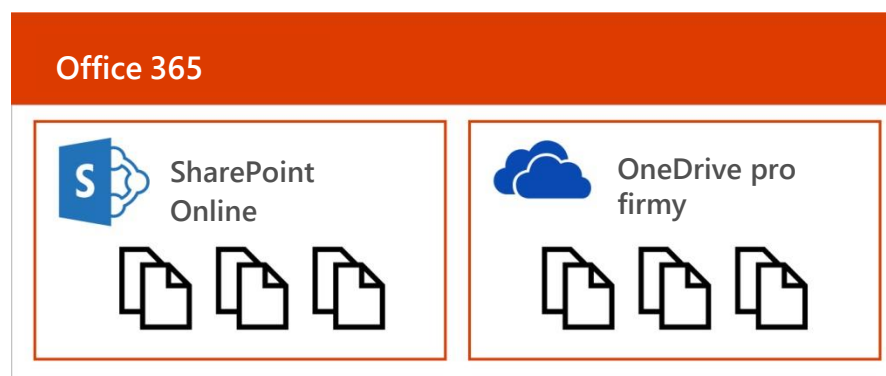
Řada organizací podporuje spolupráci tím, že umožňují externí sdílení. Zjistěte, jak máte nakonfigurována nastavení na úrovni tenantu. Poté zkontrolujte nastavení externího sdílení u webů obsahujících osobní údaje.

Externí uživatel je člověk mimo vaši organizaci, který dostane pozvání k přístupu k vašim webům a dokumentům na SharePointu Online, ale nemá licenci na vaše předplatné služeb SharePoint Online nebo Microsoft Office 365.

Zásady externího sdílení platí pro knihovny SharePointu i OneDrivu pro firmy.

Ke konfiguraci zásad sdílení musíte mít na SharePointu Online oprávnění správce.

Pokud chcete sdílet web nebo dokument s externími uživateli, musíte být vlastníkem webu nebo mít oprávnění Úplné řízení.



Typ sdílení	Co mohou externí uživatelé dělat	Oznámení
<ul style="list-style-type: none"> Sdílení mimo organizaci není povoleno Sdílení je povoleno pouze s ověřenými externími uživateli (lze povolit přidávání nových nebo omezit na stávající) Je povoleno sdílení s externími uživateli, kteří mají odkaz pro anonymní přístup Omezení externího sdílení pomocí domén (seznam povolených a zakázaných) Volba výchozího typu odkazu (anonymní, s možností sdílení v rámci společnosti, omezený) <p>Tyto zásady (v modrém poli) lze nastavit pro jednotlivé kolekce webů.</p>	<ul style="list-style-type: none"> Externí uživatelé nemohou sdílet soubory, složky a weby, které nevládní Od externích uživatelů je vyžadováno, aby pozvánku ke sdílení přijali pomocí účtu, na který byla odeslána 	<p>Momentálně k dispozici pouze na OneDrivu pro firmy. Upozornit vlastníky, když:</p> <ul style="list-style-type: none"> Uživatelé pozvou ke sdíleným souborům další externí uživatele Externí uživatelé přijmou pozvánku k přístupu k souborům Je vytvořen nebo změněn odkaz pro anonymní přístup

[Správa externího sdílení v prostředí SharePointu Online](#)
[Sdílení webů nebo dokumentů s lidmi mimo vaši organizaci](#)

Zásady přístupu k zařízením na úrovni webu

SharePoint Online a OneDrive pro firmy umožňují konfigurovat zásady přístupu k zařízením na úrovni webu. Můžete tak posílit ochranu webů obsahujících citlivá data.

Zásady přístupu k zařízením na úrovni webu při konfiguraci nezapomeňte zkoordinovat se zásadami na úrovni tenantu a také se zásadami přístupu nakonfigurovanými ve službách Azure Active Directory, Intune a Intune App Management.

[Centrum pro správu SharePointu Online: Řízení přístupu z nespravovaných zařízení](#)

Zásady přístupu k zařízením ve službách SharePoint a OneDrive pro firmy vyžadují podle scénáře, který implementujete, podpůrné zásady ve službách Azure Active Directory a Microsoft Intune. Viz tabulku níže.

Scénáře a závislosti pro přístup k zařízením

Cíl	Povolit přístup pouze z umístění s konkrétními IP adresami	Zabránit uživatelům ve stahování souborů ze zařízení nepřipojených k doméně	Blokovat přístup ze zařízení nepřipojených k doméně	Zabránit uživatelům ve stahování souborů do zařízení neodpovídajících předpisům	Blokovat přístup ze zařízení neodpovídajících předpisům
Centrum pro správu SharePointu	✓	✓	✓	✓	✓
Azure Active Directory		✓	✓	✓	✓
Microsoft Intune				✓	✓

Ochrana přístupu ke službám pro identity a zařízení

Microsoft doporučuje nakonfigurovat ochranu identit a zařízení, která mají ke službě přístup. Úsilí, které vložíte do ochrany přístupu ke službám Office 365, lze zúročit při ochraně dalších služeb typu SaaS nebo PaaS a dokonce i aplikací jiných poskytovatelů cloudových služeb.

Ochrana přístupu identit a zařízení představuje základní úroveň ochrany zajišťující, že identity nebudou narušeny, zařízení budou v bezpečí a data organizace, k nimž mají zařízení přístup, budou izolována a chráněna.

Úvodní doporučení a pokyny ke konfiguraci najdete v článku [Bezpečnostní pokyny Microsoftu pro politické kampaně, neziskové organizace a další agilní organizace](#).

Pokyny pro prostředí s hybridními identitami a službou AD FS najdete v článku [Doporučené bezpečnostní zásady a konfigurace](#).

Cloudové služby

Služba Azure Active Directory zajišťuje přístup na základě identit k libovolné cloudové službě, včetně služeb jiných cloudových poskytovatelů než Microsoft, jako je Amazon Web Services.

Typy účtů

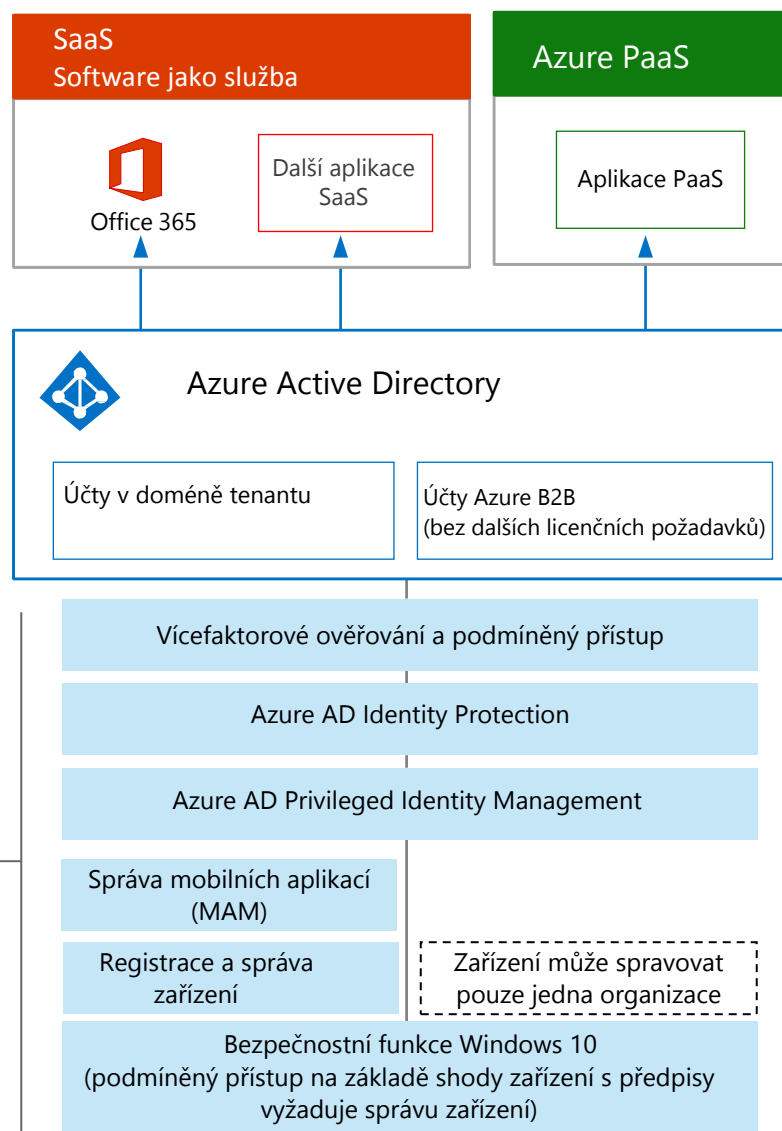
Účty v doméně tenantu – účty, které přidáte do tenantu a spravujete přímo.

Účty B2B – účty pro uživatele mimo vaši organizaci, které přivzete ke spolupráci. Může jít o jiné účty Office 365, účty jiné organizace nebo spotřebitelské účty (například Gmail).

Funkce

Tyto funkce chrání identity a zařízení. Schéma vedle shrnuje funkce dostupné pro jednotlivé typy účtů.

Funkce ve sloupci B2B jsou dostupné bez dalších licencí. Podle potřeby můžete k B2B účtům přidat licence a poskytnout jejich uživatelům další funkce a zároveň chránit přístup k osobním údajům ve vašem prostředí.



Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

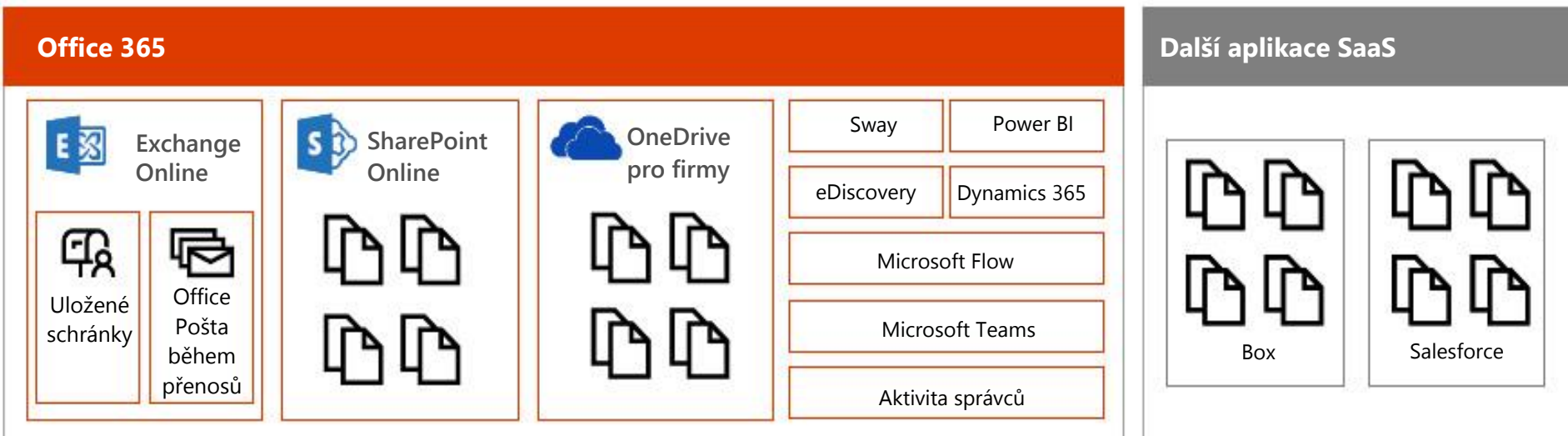
Toto je 6. téma ze sedmidílné série.



Monitorování úniků osobních údajů

K monitorování použití a přenosů osobních údajů lze využít celou řadu nástrojů. Toto téma popisuje tři z nich, které se dobře osvědčují.

Nástroje doporučené pro monitorování osobních údajů v Office 365 a dalších aplikacích SaaS



Microsoft Cloud App Security

Sestavy ochrany před únikem informací v Office 365

Protokol auditování a zásady upozornění v Office 365

1 Začněte sestavami ochrany před únikem informací v Office 365, které umožňují monitorování osobních údajů na SharePointu Online, OneDrive pro firmy a v e-mailových zprávách během přenosů. Tyto sestavy nabízejí nejpodrobnější úroveň monitorování osobních údajů.

2 Zásady upozornění a protokol auditu v Office 365 slouží k monitorování aktivity ve službách Office 365. Můžete nastavit průběžné monitorování nebo cíleně prohledávat protokol auditu při prošetřování incidentů.

3 Služba Cloud App Security slouží k monitorování souborů obsahujících citlivá data u dalších poskytovatelů SaaS. Připravujeme možnost používat typy citlivých informací v Office 365 a sjednocené popisky v prostředích Azure Information Protection a Office. Můžete nastavit zásady platné pro všechny aplikace SaaS (včetně Office 365) nebo pro konkrétní aplikace (například Box).

Sestavy ochrany před únikem informací v Office 365

Jakmile vytvoříte zásady ochrany před únikem informací (DLP), je třeba ověřit, zda fungují podle vašeho záměru a pomáhají vám zajistit soulad s předpisy. V sestavách DLP v Office 365 můžete rychle zkontrolovat počet shod se zásadami DLP, počet přepsání či falešně pozitivních výsledků, zjistit, jak se jejich trendy vyvíjejí v čase, různě sestavu filtrovat a zobrazit další podrobnosti k vybranému bodu na čáře v grafu.

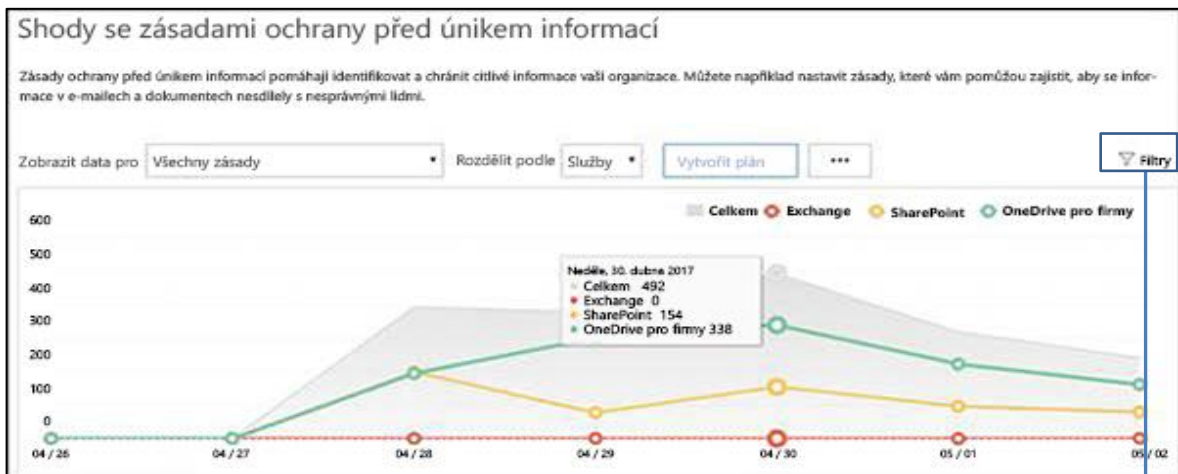
Možnosti využití sestav DLP:

- Zaměření na konkrétní období a analýza příčin výkyvů a trendů
- Odhalení obchodních procesů porušujících zásady DLP ve vaší organizaci
- Analýza obchodních dopadů zásad DLP
- Zobrazení odůvodnění zadaných uživateli, když řeší upozornění na možný únik citlivých informací přepsáním zásady nebo ohlášením falešně pozitivního výsledku
- Ověření dodržování konkrétní zásady DLP zobrazením veškerých shod s touto zásadou
- Zobrazení seznamu souborů obsahujících citlivá data, které odpovídají vašim zásadám DLP, v podokně detailů

Navíc můžete sestavy DLP využít k tomu, abyste během spouštění v testovacím režimu zásady DLP vyladili.

Sestavy DLP jsou k dispozici v Centru zabezpečení a dodržování předpisů. Přejděte do části **Sestavy** > **Zobrazit sestavy**. V části **Ochrana před únikem informací (DLP)** přejděte na **Shody se zásadami a pravidly ochrany před únikem informací** nebo na **Falešně pozitivní výsledky a přepsání zásad ochrany před únikem informací**.

Další informace najdete v článku [Zobrazení sestav ochrany před únikem informací](#).



Filtry

Datum

Datum zahájení: 2017-12-06

Datum ukončení: 2017-12-12

Služby

- SharePoint
- OneDrive pro firmy
- Exchange

Použit **Zrušit**

Protokol auditování a zásady upozornění v Office 365

Protokol auditování Office 365 obsahuje události ze služeb Exchange Online, SharePoint Online, OneDrive pro firmy, Azure Active Directory, Microsoft Teams, Power BI, Sway a dalších služeb Office 365.

Centrum zabezpečení a dodržování předpisů Office 365 nabízí dva způsoby, jak protokol auditování Office 365 monitorovat a generovat na jeho základě sestavy:

- **Nastavení zásad upozornění, zobrazení upozornění a monitorování trendů** – Využijte nové zásady upozornění a nástroje na řídicích panelech upozornění v Centru zabezpečení a dodržování předpisů Office 365.
- **Přímé prohledávání protokolu auditování** – Vyhledejte všechny události v zadaném rozsahu dat. Nebo můžete výsledky filtrovat podle určitých kritérií, například podle uživatele, který akci provedl, podle akce nebo cílového objektu.

Týmy pro zabezpečení informací a dodržování předpisů mohou tyto nástroje využít k proaktivní kontrole činností, které ve službách Office 365 provádějí koncoví uživatelé i správci. Automatická upozornění lze nakonfigurovat tak, aby odeslala oznámení e-mailem, pokud ve specifické kolekci webů dojde k určitým aktivitám – například při sdílení obsahu z webů, které obsahují informace související s nařízením GDPR. Specializované týmy pak mohou kontaktovat uživatele a ověřit, zda dodržují podnikové zásady zabezpečení, případně doplnit potřebná školení.

Týmy pro zabezpečení informací mohou protokol auditování prohledávat také při šetření podezření na úniky dat, kdy pomáhá určit příčinu i rozsah útoku. Tato integrovaná funkce usnadňuje dodržení článků 33 a 34 nařízení GDPR, jež vyžadují oznámit porušení zabezpečení v určité časové lhůtě dozorovému úřadu GDPR a samotnému subjektu údajů. Záznamy v protokolu auditování se ve službě uchovávají pouze 90 dnů – často se doporučuje uchovávat je déle a u mnoha organizací je to přímo vyžadováno.

K dispozici jsou řešení, jež umožňují odebírat sjednocené protokoly auditu prostřednictvím rozhraní Microsoft Management Activity API a dokážou podle potřeby ukládat protokoly záznamů i zajistit podrobné řídicí panely a upozornění. Příkladem je řešení [Microsoft Operations Management Suite \(OMS\)](#).

Další informace o zásadách upozornění a vyhledávání v protokolu auditování:

[Zásady upozornění v Centru zabezpečení a dodržování předpisů Office 365](#)

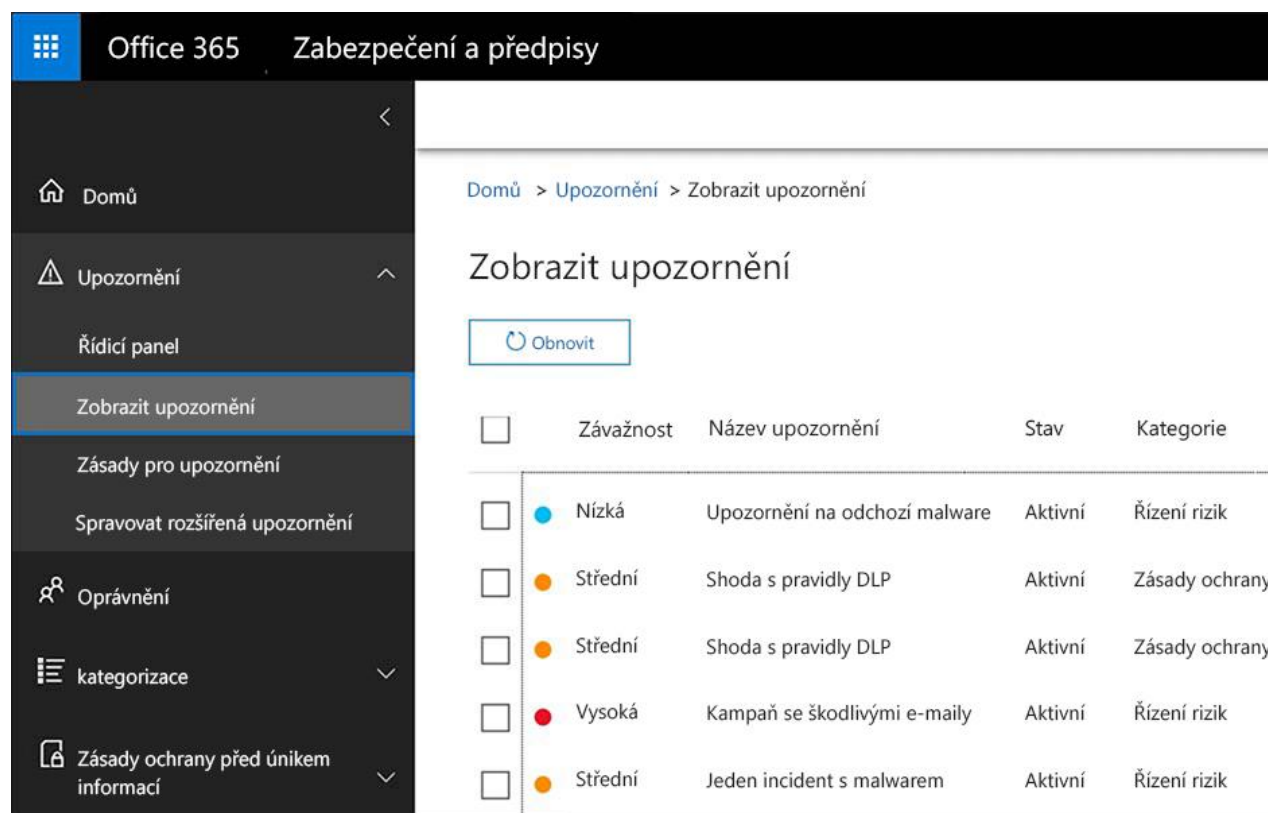
[Vyhledávání aktivity správců a uživatelů v protokolu auditování v Office 365](#) (úvod)

[Zapnutí a vypnutí vyhledávání v protokolu auditu v Office 365](#)

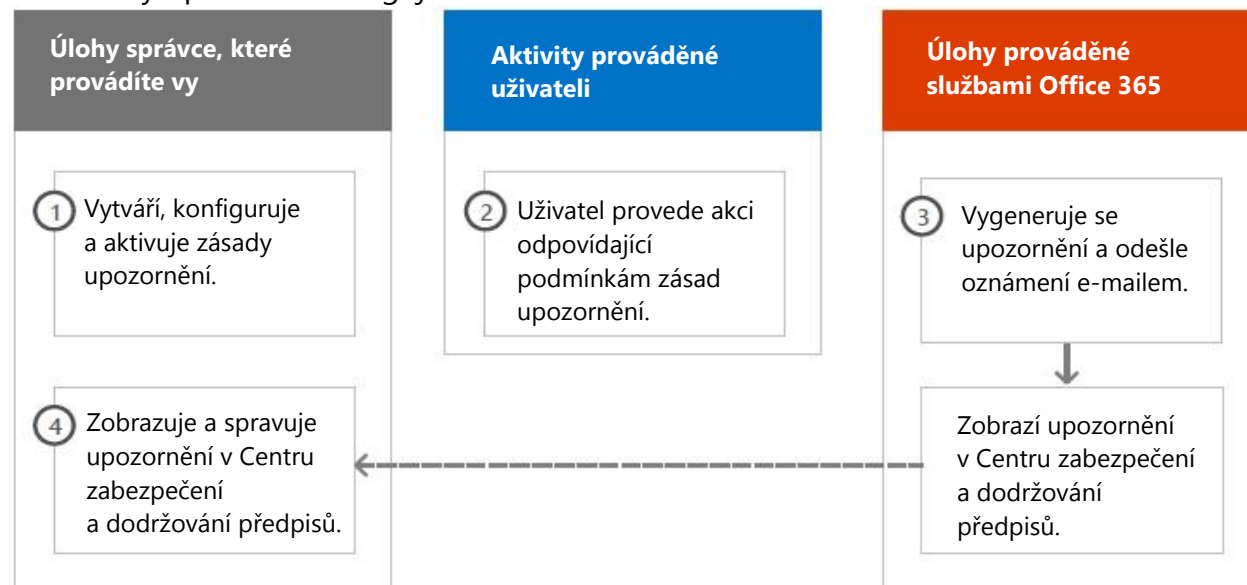
[Vyhledávání v protokolu auditování v Centru zabezpečení a dodržování předpisů Office 365](#)

[Search-UnifiedAuditLog](#) (rutina)

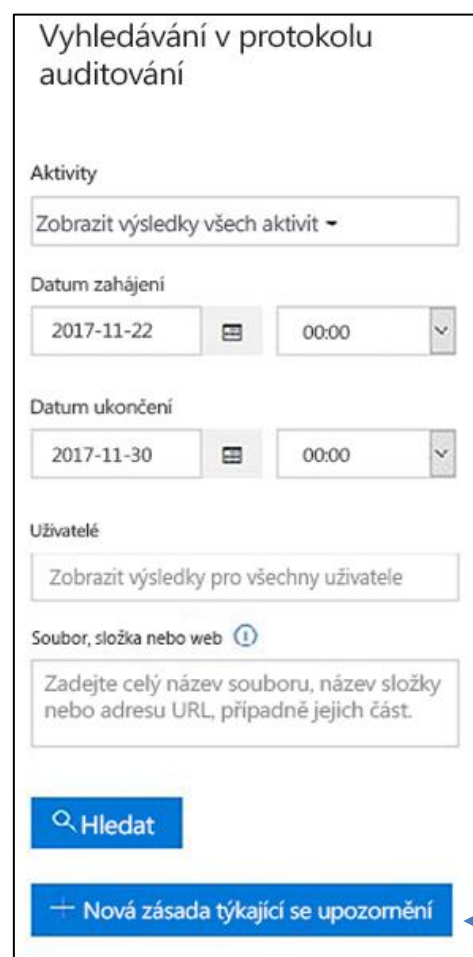
[Podrobné vlastnosti v protokolu auditu v Office 365](#)



Jak zásady upozornění fungují



Hledání v protokolu auditování



Příklady aktivit souvisejících s nařízením GDPR:

- Zobrazení souboru
- Zkopírování souboru
- Stažení souboru
- Přijetí žádosti o přístup
- Přijetí pozvánky ke sdílení
- Přerušení dědičnosti úrovní oprávnění
- Vytvoření anonymního odkazu
- Vytvoření pozvánky ke sdílení
- Povolení synchronizace souborů v počítači
- Stažení souborů do počítače
- Změna zásad sdílení (správce webu)
- A mnoho dalších

Vyhledávání můžete omezit na weby, o kterých víte, že obsahují osobní údaje.

Vytvořte zásady upozornění pro průběžné monitorování konkrétních aktivit. Jedná se o odlišné zásady, než jsou zásady upozornění na novém řídicím panelu Upozornění. Tato upozornění se odesílají určeným příjemcům. Již vytvořené zásady můžete prohlížet v prostředí PowerShell.

Výsledky hledání v protokolu auditování

Datum	Uživatel	Položka	Detail
2015-09-21 16:48:33	správce		
2015-09-21 16:49:16	správce	admin_contoso_com_SThumb.jpg	Zobrazeno v Fotografie uživatele/Pro...
2015-09-21 16:49:28	admin@contoso.com	Zobrazení souboru	Spustit sestavu aktivit Office 365... Zobrazeno v Dokumenty
2015-09-21 16:49:28	admin@contoso.com	Stažení souboru	Spustit sestavu aktivit Office 365... Staženo z Dokumenty
2015-09-21 16:49:44	v-temp@contoso.com	Zobrazení souboru	Mzdy_IT_odd.docx Zobrazeno v Pouze_mgmt_IT
2015-09-21 16:50:27	ping@contoso.com	Změna souboru	Olympics (Sample).xlsx Změněno v Dokumenty
2015-09-21 16:50:28	admin@contoso.com	Přejmenování souboru	Auditování – Exchange2.pptx Přejmenováno na Auditování_finální

Po dokončení vyhledávání se zobrazí počet nalezených výsledků.

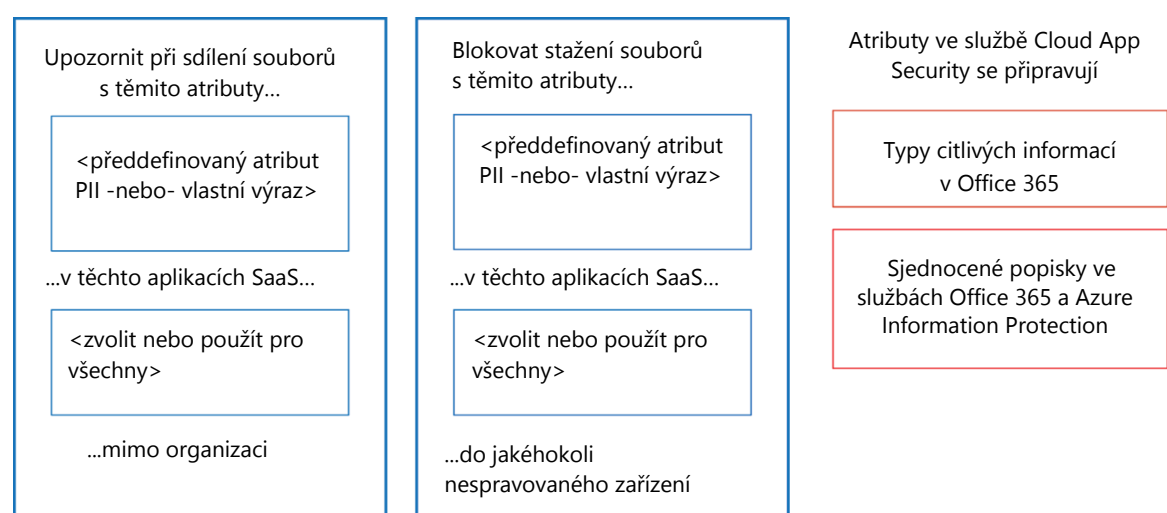
Microsoft Cloud App Security

Služba Microsoft Cloud App Security pomáhá vyhledat další aplikace SaaS, které se používají ve vašich sítích a přijímají nebo odesílají citlivá data.

Microsoft Cloud App Security je ucelená služba, které poskytuje detailní přehled, podrobné kontrolní mechanismy a vylepšenou ochranu před hrozbami pro cloudové aplikace. Rozpozná více než 15 000 cloudových aplikací ve vaší síti, a to ze všech zařízení, a poskytuje hodnocení rizik a jejich průběžné posuzování a analýzu. Nevyžaduje žádné agenty, protože informace potřebné k získání celkového přehledu a souvislostí o používání cloudu a stínovém IT shromažďuje z bran firewall a proxy serverů.

Prošetřovací funkce služby Cloud App Security nabízí podrobné informace o všech aktivitách, souborech a účtech pro schválené a spravované aplikace, takže získáte lepší přehled o vašem cloudovém prostředí. Můžete získat podrobné informace na úrovni souborů a mapovat pohyb dat v cloudových aplikacích.

Zásady služby Cloud App Security užitečné pro soulad s nařízením GDPR



Řídicí panel služby Cloud App Security

Pokud jste službu Cloud App Security ještě nezačali používat, nejprve ji spusťte.

Služba Cloud App Security je dostupná na adrese <https://portal.cloudappsecurity.com>.

Poznámka: Po spuštění služby Cloud App Security nebo před přiřazením popisků nezapomeňte aktivovat volbu **'Automaticky v nových souborech vyhledávat popisky kategorizace Azure Information Protection'**. Po prvotním nastavení služba Cloud App Security znovu neprohledává existující soubory, dokud nejsou upraveny.

[Nasazení služby Cloud App Security](#)

[Další informace o službě Microsoft Cloud App Security](#)

[Blokování stahování citlivých informací pomocí funkce proxy služby Microsoft Cloud App Security](#)

Příklad zásad pro soubory a aktivity k rozpoznání sdílení osobních údajů

Poznámka: Tyto zásady vyžadují funkce, které jsou momentálně dostupné ve verzi Private Preview.

Rozpoznání sdílení souborů obsahujících informaci PII – číslo platební karty	
Upozornit na sdílení souboru obsahujícího číslo platební karty ze schválené cloudové aplikace	
Ovládací prvek	Nastavení
Typ zásady	Zásady pro soubory
Šablona zásady	Bez šablony
Závažnost zásady	Vysoká
Kategorie	DLP
Nastavení filtru	Úroveň přístupu = Veřejný (internet), Veřejný, Externí aplikace = <vyberte aplikace> (toto nastavení použijte, pokud chcete monitorování omezit na konkrétní aplikace SaaS)
Použít na	Všechny soubory, všichni vlastníci
Kontrola obsahu	<ul style="list-style-type: none"> Zahrnuje soubory odpovídající výrazu: Všechny země: Finanční: Číslo kreditní karty Nevyžadovat relevantní kontext: nezaškrtnuto (bude se vyhledávat shoda s regulárním výrazem i klíčovými slovy) Zahrnuje soubory s alespoň 1 shodou Zrušit maskování posledních 4 znaků porušení: zaškrtnuto
Upozornění	<ul style="list-style-type: none"> Vytvořit upozornění pro každý odpovídající soubor: zaškrtnuto Denní limit upozornění: 1000 Poslat upozornění jako e-mail: zaškrtnuto Komu: infosec@contoso.com
Řízení	Microsoft OneDrive pro firmy <ul style="list-style-type: none"> Nastavit jako soukromé: zaškrtnuto políčko Odebrat externí uživatele <ul style="list-style-type: none"> Všechna ostatní nastavení: nezaškrtnuto Microsoft SharePoint Online <ul style="list-style-type: none"> Nastavit jako soukromé: zaškrtnuto políčko Odebrat externí uživatele Všechna ostatní nastavení: nezaškrtnuto

Rozpoznání údajů o zákaznících nebo personálních údajů ve službách Box nebo OneDrive pro firmy	
Upozornění v případě, že je do služby Box nebo OneDrive pro firmy nahrán soubor s popiskem Údaje o zákaznících nebo Personální údaje	
Poznámka: K monitorování služby Box je nutné nakonfigurovat konektor pomocí sady API Connector SDK.	
Ovládací prvek	Nastavení
Typ zásady	Zásada pro aktivitu
Šablona zásady	Bez šablony
Závažnost zásady	Vysoká
Kategorie	Řízení sdílení
Pracovat s	Jedna aktivita
Nastavení filtru	<ul style="list-style-type: none"> Typ aktivity = Nahrání souboru Aplikace = Microsoft OneDrive pro firmy a Box Popisek kategorizace (aktuálně ve verzi Private Preview): Azure Information Protection = Údaje o zákaznících, Personální oddělení – údaje o mzdách, Personální oddělení – údaje o zaměstnancích
Upozornění	<ul style="list-style-type: none"> Vytvořit upozornění: zaškrtnuto Denní limit upozornění: 1000 Poslat upozornění jako e-mail: zaškrtnuto Komu: infosec@contoso.com
Řízení	Všechny aplikace <ul style="list-style-type: none"> Umístit uživatele do karantény: zaškrtnuto Všechna ostatní nastavení: nezaškrtnuto Office 365 <ul style="list-style-type: none"> Umístit uživatele do karantény: zaškrtnuto Všechna ostatní nastavení: nezaškrtnuto

Podobné zásady:

- **Rozpoznání sdílení souborů obsahujících informaci PII – e-mailová adresa**
- **Rozpoznání sdílení souborů obsahujících informaci PII – číslo pasu**

Podobné zásady:

- **Rozpoznání rozsáhlého stahování údajů o zákaznících nebo personálních údajů** – Upozornit v případě, kdy je zjištěno, že jeden uživatel v krátké době stáhl velké množství souborů obsahujících údaje o zákaznících nebo personální údaje
- **Rozpoznání sdílení údajů o zákaznících nebo personálních údajů** – Upozornění na sdílení souborů obsahujících údaje o zákaznících nebo personální údaje

Ochrana informací ve službách Office 365 s ohledem na nařízení GDPR

Architektura ochrany citlivých informací v Office 365

Toto je 7. téma ze sedmidílné série.



Použití služby Compliance Manager na portálu Service Trust Portal

Služba Compliance Manager na portálu [Microsoft Service Trust Portal](#) (STP) poskytuje nástroje ke sledování, implementaci a správě kontrolních mechanismů auditování, které vaši organizaci pomohou dosáhnout shody s oborovými standardy zabezpečení nebo ochrany dat posuzované v cloudových službách Microsoft, jako je Office 365 a Microsoft Azure. Zaměstnanci pověřenému dohledem nad ochranou osobních údajů (někdy přímo na specializované pozici) tato služba pomáhá řídit proces zajišťování shody a vyhodnocování rizik.

[Služba Compliance Manager na portálu Service Trust Portal \(servicetrust.microsoft.com\)](#)

[Použití služby Compliance Manager na portálu Service Trust Portal](#)

[Blog TechNet: Seznámení s novým portálem Service Trust Portal](#)

[Blogový příspěvek: Služba Compliance Manager je nově dostupná ve verzi Preview](#)

[Blogový příspěvek: Správa souladu s předpisy na jednom místě – Představujeme službu Compliance Manager](#)

Compliance Manager

- Spojuje podrobné informace poskytované společností Microsoft auditorům a úřadům v rámci auditů cloudových služeb Microsoftu různými třetími stranami ověřujícími soulad s různými normami a standardy (jako jsou normy ISO 27001:2013 a ISO 27018:2014) a informace, které Microsoft shromažďuje interně pro účely vlastního souladu s předpisy (jako je obecné nařízení EU o ochraně osobních údajů GDPR) s vaším vlastním hodnocením toho, jak tyto standardy a nařízení dodržuje vaše organizace.
- Umožňuje vám přiřazovat, sledovat a vykazovat činnosti související s hodnocením, což vám v organizaci může pomoci překročit překážky mezi týmy a naplnit cíle organizace v oblasti souladu s předpisy.
- Poskytuje bezpečné úložiště pro nahrávání a správu dokladů a dalších prvků souvisejících s činností v oblasti souladu s předpisy.
- Umožňuje vytvářet v Microsoft Excelu bohaté a podrobné sestavy dokumentující činnost v oblasti souladu s předpisy ze strany Microsoftu i vaší organizace, které lze poskytnout auditorům, úřadům a dalším zainteresovaným stranám.

Základní součástí služby Compliance Manager je Posouzení. To spojuje cloudovou službu Microsoftu (jako je Office 365) se standardem certifikace nebo nařízením na ochranu osobních údajů (jako je GDPR). Posouzení vám umožňují srovnat postoj k ochraně osobních údajů a shodě s předpisy ve vaší organizaci s vybraným oborovým standardem pro vybranou cloudovou službu Microsoft. Posouzení jsou završena implementací kontrolních mechanismů odpovídajících posuzovanému standardu.

Každé posouzení zahrnuje:

- **Kontrolní mechanismy spravované Microsoftem** – U každého kontrolního mechanismu spravovaného Microsoftem poskytne služba Compliance Manager podrobnosti o tom, jak společnost Microsoft kontrolní mechanismus implementovala, včetně informace, kdy byl otestován a ověřen nezávislým auditorem.
- **Kontrolní mechanismy spravované zákazníkem** – Za implementaci těchto kontrolních mechanismů odpovídá v rámci procesu zajištění shody s daným standardem či nařízením vaše organizace.



Compliance Manager je řídicí panel, který nabízí souhrn stavu ochrany osobních údajů a souladu s předpisy a doporučení, jak je zlepšit. Jedná se skutečně pouze o doporučení, vyhodnocení jejich efektivity před nasazením ve vašem prostředí je na vás. Doporučení služby Compliance Manager nelze chápat jako záruku dodržování předpisů.

U každého kontrolního mechanismu spravovaného zákazníkem...

- 1 Přiřaďte položku dalšímu uživateli zodpovědnému za patřičné kroky.
- 2 Nahrajte dokumenty a další doklady související s úlohou implementace.
- 3 Přidejte kroky implementace, které vaše organizace podnikla směrem ke splnění požadavků.
- 4 Nastavte stav na **Neimplementováno**, **Implementováno**, **Alternativní implementace**, **Plánováno** nebo **Mimo rozsah**.
- 5 Zadejte datum testu a výsledek: **Neposouzeno**, **Vyhovuje**, **Nevyhovuje – nízké riziko**, **Nevyhovuje – střední riziko**, **Nevyhovuje – vysoké riziko**.

Kliknutím na „Další informace“ se dozvíte podrobnosti o akcích, které Microsoft doporučuje k jednotlivým článkům.