Příprava na obecné nařízení o ochraně osobních údajů (GDPR)

Dosáhněte rychleji souladu s nařízením GDPR pomocí služby Microsoft Cloud

Obsah

Zřeknutí se práv

Tato informační brožura obsahuje komentář k obecnému nařízení o ochraně osobních údajů, který vysvětluje přístup společnosti Microsoft a je aktuální ke dni zveřejnění. Strávili jsme velké množství času studováním nařízení GDPR a domníváme se, že jsme při rozboru jeho záměru a významu byli dostatečně pečliví. Uplatnění nařízení GDPR v praxi však ve vysoké míře závisí na konkrétní situaci a ne všechny aspekty a interpretace nařízení GDPR lze považovat za zcela ustálené.

V důsledku toho poskytujeme tuto informační brožuru pouze pro informační účely, a nelze ji tak považovat za zdroj právního poradenství ani za návod, jak můžete vy nebo vaše organizace aplikovat obecné nařízení o ochraně osobních údajů. Při projednávání nařízení GDPR, postupu jeho specifické aplikace ve vaší organizaci a způsobu, jak nejlépe zajistit soulad s tímto nařízením, vám doporučujeme spolupracovat s odborníkem v oblasti práva.

SPOLEČNOST MICROSOFT NEPOSKYTUJE NA INFORMACE UVEDENÉ V TÉTO INFORMAČNÍ BROŽUŘE VÝSLOVNĚ UVEDENÉ, IMPLICITNĚ PŘEDPOKLÁDANÉ ANI ZÁKONNÉ ZÁRUKY. Tato informační brožura je poskytována „tak, jak je“. Informace a pohledy uvedené v tomto dokumentu, včetně adres URL a dalších odkazů na internetové weby, mohou být změněny bez předchozího upozornění.

Publikováno v květnu 2017

Verze 1.1

Úvod

Dne 25. května 2018 nabude účinnosti evropský zákon o ochraně osobních údajů, který stanoví nová globální pravidla pro práva na ochranu soukromí, zabezpečení a zajištění souladu.

Obecné nařízení o ochraně osobních údajů (GDPR, General Data Protection Regulation) se v zásadě týká ochrany a zajištění práv jednotlivců na ochranu soukromí. Definuje přísné globální požadavky ohledně ochrany osobních údajů, které řídí správu a ochranu osobních údajů při současném respektování individuální volby bez ohledu na to, kam jsou data odesílána a kde jsou zpracovávána nebo ukládána.

Společnost Microsoft a její zákazníci se vydali na cestu za dosažením cílů ochrany osobních údajů stanovených nařízením GDPR. Domníváme se, že ochrana osobních údajů je základním právem, a věříme, že nařízení GDPR představuje důležitý krok vpřed, pokud jde o vyjasnění a zajištění práv jednotlivců na ochranu soukromí. Současně si ale uvědomujeme, že nařízení GDPR vyžaduje, aby společnosti po celém světě provedly významné změny.

Splnění požadavků nařízení GDPR se vám může zdát jako velmi náročný úkol, a proto jsme zde, abychom vám pomohli.

Závazek společnosti Microsoft v souvislosti s nařízením GDPR

Základním kamenem naší snahy pomoci každé osobě a každé organizaci na této planetě dosáhnout vyšších cílů je důvěra. Při budování této důvěry se řídíme principiálním přístupem se silným důrazem na ochranu soukromí, zabezpečení, soulad s předpisy a transparentnost. Právě tyto principy uplatňujeme při přípravě na obecné nařízení o ochraně osobních údajů.

Uvědomujeme si, že zajištění souladu s nařízením GDPR je sdílenou odpovědností. Z tohoto důvodu jsme se zavázali zajistit soulad s nařízením GDPR napříč všemi našimi cloudovými službami dříve, než toto nařízení nabude 25. května 2018 účinnosti.

Zavázali jsme se také, že se podělíme o naše zkušenosti se zajišťováním souladu se složitými předpisy, abychom vám pomohli najít nejlepší cestu pro vaši organizaci ke splnění požadavků ochrany osobních údajů stanovených nařízením GDPR. Prostřednictvím nejkomplexnější sady nabídek pro zajištění souladu a zabezpečení od libovolného poskytovatele cloudu a rozsáhlého ekosystému partnerů jsme připraveni podpořit vaše iniciativy související s ochranou osobních údajů a zabezpečením, a to jak dnes, tak i v budoucnosti.

Jako součást našeho závazku stát se vaším partnerem na cestě za splněním požadavků nařízení GDPR jsme vytvořili tuto informační brožuru, která vám pomůže s přípravami. Brožura poskytuje přehled nařízení GDPR, popisuje, jak se na ně připravujeme, a nabízí příklady kroků, které můžete učinit již dnes s pomocí společnosti Microsoft, abyste se vydali na vlastní cestu směřující k zajištění souladu s nařízením GDPR.

Těšíme se, až budeme moci sdílet další aktualizované informace o tom, jak vám můžeme pomoci vyhovět tomuto důležitému novému zákonu a současně zdokonalit ochranu osobních údajů. Navštivte naši sekci Centra zabezpečení Microsoft věnovanou nařízení GDPR, ve které naleznete další materiály a dozvíte se více o tom, jak vám společnost Microsoft může pomoci splnit specifické požadavky nařízení GDPR.

Úvodní seznámení s nařízením GDPR

Než vás seznámíme s konkrétními cestami zajištění souladu s obecným nařízením o ochraně osobních údajů, které vám společnost Microsoft může pomoci připravit, rádi bychom nabídli odpovědi na některé z nejzákladnějších a nejkritičtějších otázek týkajících se nařízení a případných důsledků pro vás. Podrobnější přehled najdete zde.

Co je obecné nařízení o ochraně osobních údajů?

Nařízení GDPR je nové nařízení o ochraně osobních údajů platné pro celou Evropskou unii. Poskytuje jednotlivcům větší kontrolu nad jejich osobními údaji, zajišťuje transparentnost ohledně používání dat a vyžaduje zabezpečení a opatření pro ochranu dat.

Vztahuje se obecné nařízení o ochraně osobních údajů na naši organizaci?

Nařízení GDPR má mnohem širší záběr, než by se mohlo na první pohled zdát. Tento zákon zavádí nová pravidla pro společnosti, orgány státní správy a neziskové nebo další organizace, které nabízejí zboží a služby lidem v Evropské unii (EU) nebo které shromažďují a analyzují data úzce související s obyvateli EU, a platí pro organizace, které byly založeny v Evropské unii (EU), nabízejí zboží nebo služby v EU nebo monitorují chování obyvatel EU. Nařízení GDPR se na vás vztahuje bez ohledu na vaše umístění.

Na rozdíl od zákonů o ochraně osobních údajů v některých jiných jurisdikcích se nařízení GDPR vztahuje na organizace všech velikostí a ze všech odvětví. EU je často považována za vzor pro mezinárodní řešení problémů ochrany osobních údajů, takže očekáváme, že principy obsažené v nařízení GDPR budou časem přijaty v dalších částech světa.

Kdy nabude obecné nařízení o ochraně osobních údajů účinnosti?

Obecné nařízení o ochraně osobních údajů nabude účinnosti 25. května 2018 a nahradí stávající směrnici o ochraně dat (směrnice 95/46/ES), která platí od roku 1995. Nařízení GDPR se ve skutečnosti stalo zákonem v EU v dubnu 2016, ale vzhledem k významným změnám, které budou muset některé organizace provést, aby vyhověly požadavkům nařízení, bylo zavedeno dvouleté přechodné období.

Jaké hlavní principy obecné nařízení o ochraně osobních údajů obsahuje?

Nařízení GDPR je založeno na šesti principech:

- Vyžadování transparentnosti při manipulaci s osobními údaji a používání osobních údajů
- Omezení zpracovávání osobních údajů pouze na stanovené a opodstatněné účely
- Omezení shromažďování a ukládání osobních údajů pouze na zamýšlené účely
- Umožnění jednotlivcům provádět opravy svých osobních údajů nebo vyžadovat jejich odstranění
- Omezení ukládání dat obsahujících osobní údaje pouze na dobu nezbytnou pro zamýšlený účel
- Zajištění ochrany osobních údajů pomocí náležitých postupů zabezpečení

Jaké jsou příklady požadavků obecného nařízení o ochraně osobních údajů v souvislosti s těmito principy?

- Podle obecného nařízení o ochraně osobních údajů mají jednotlivci právo vědět, zda organizace zpracovává jejich osobní údaje, a seznámit se s účelem tohoto zpracování. Libovolný jednotlivec má právo požadovat odstranění svých údajů nebo jejich opravu, požadovat, aby již nebyly jeho údaje zpracovávány, ohradit se proti přímému marketingu a odvolat souhlas s určitým používáním svých údajů. Právo na přenositelnost dat poskytuje jednotlivcům právo na přesunutí jejich údajů na jiné místo a získat pomoc, pokud tak chtějí učinit.
- Nařízení GDPR vyžaduje od organizací, aby zabezpečily osobní údaje podle jejich citlivosti. V případě narušení zabezpečení dat musí správci dat obvykle informovat příslušné orgány do 72 hodin. Navíc pokud takové narušení zabezpečení může se značnou pravděpodobností vést k vysokému stupni nebezpečí pro práva a svobody jednotlivců, musí organizace také bez zbytečného odkladu oznámit tuto skutečnost postiženým jednotlivcům.
- Zpracování osobních údajů musí mít právní základ. Veškerá svolení ke zpracování osobních údajů musí být poskytnuta „dobrovolně, konkrétně, kvalifikovaně a jednoznačně“. Nařízení GDPR obsahuje specifické požadavky na vyjádření souhlasu, jejichž cílem je zajistit ochranu dětí.

- Organizace musí vyhodnocovat dopad ochrany dat, aby mohly předpovídat dopad projektů na ochranu osobních údajů a podle potřeby zavádět zmírňující opatření. Je nutné uchovávat záznamy o aktivitách zpracování, souhlasech se zpracováním dat a souladu s nařízením GDPR.
- Zajištění souladu s nařízením GDPR není jednorázová aktivita, ale probíhající proces. Nedodržení požadavků nařízení GDPR může vést k významným finančním postihům. V zájmu zajištění souladu s nařízením GDPR je organizacím doporučováno, aby přijaly kulturu ochrany osobních údajů, a chránily tak zájmy jednotlivců ohledně jejich osobních údajů.

Podrobnější přehled informací o nařízení GDPR najdete na adrese Microsoft.com/GDPR. Zde jsou také pro lepší pochopení vysvětleny pojmy jako pseudonymizace, zpracování, správci, zpracovatelé, subjekty údajů a osobní údaje. Jsme odhodláni pomoci vám splnit požadavky nařízení GDPR a dále podporovat práva jednotlivců na ochranu osobních údajů.

Partnerství se společností Microsoft na cestě k zajištění souladu s nařízením GDPR

Zajištění souladu s obecným nařízením o ochraně osobních údajů představuje náročný úkol pro celou firmu, který bude vyžadovat čas, nástroje, procesy a odborné znalosti a možná také významné změny ve vašich postupech ochrany osobních údajů a správy dat. Cestu ke splnění požadavků nařízení GDPR si usnadníte, pokud budete používat dobře navržený model cloudových služeb a budete mít efektivní program řízení dat. Při snaze o úspěšně splnění požadavků nařízení GDPR se můžete navíc spolehnout na pomoc společnosti Microsoft a jejího rozsáhlého partnerského ekosystému.

Společnost Microsoft se může pochlubit dlouhou historií poskytování cloudových služeb, kterým můžete důvěřovat. Přijali jsme principiální přístup k ochraně osobních údajů, zabezpečení, zajištění souladu a transparentnosti se silným důrazem na vybudování vaší důvěry v digitální technologie, na které se spoléháte. Disponujeme nejrozsáhlejším portfoliem pro zajištění souladu v oboru a jako první jsme přijali klíčové normy, jako je norma ISO/IEC 27018 o ochraně osobních údajů v cloudu. Naši zákazníci a partneři těží z našich zkušeností s vedením v oblastech ochrany osobních údajů, zabezpečení, zajištění souladu a transparentnosti.

Pokud se připravujete na splnění požadavků obecného nařízení o ochraně osobních údajů, můžeme vám nabídnout:

- **Technologie, které uspokojí vaše požadavky.** Můžete využít naše široké portfolio podnikových cloudových služeb ke splnění povinností vyplývajících z nařízení GDPR pro oblasti zahrnující odstranění, opravu, přenos a zpřístupnění osobních údajů a vyjádření nesouhlasu s jejich zpracováním. Pokud používáte technologie od společnosti Microsoft, můžete se navíc spolehnout na odbornou podporu od našeho rozsáhlého globálního partnerského ekosystému.
- **Smluvní závazky.** Stojíme za vámi prostřednictvím smluvních závazků pro naše cloudové služby, včetně včasné podpory zabezpečení a včasného reportingu v souladu s novými požadavky nařízení GDPR. V březnu 2017 byl do našich zákaznických licenčních smluv pro cloudové služby společnosti Microsoft zahrnut závazek k zajištění souladu s nařízením GDPR, jakmile nabude účinnosti.
- **Sdílení našich zkušeností.** Podělíme se o své zkušenosti získané na cestě za splněním požadavků nařízení GDPR. Budete moci využít naše poznatky a přizpůsobit si je tak, abyste vytvořili nejlepší cestu pro vaši organizaci.

Začínáme s nařízením GDPR

Přístup k nařízení GDPR založený na platformě

Systémy, které používáte k vytváření, ukládání, analýze a správě dat, lze šířit napříč širokou škálou IT prostředí, jako jsou osobní zařízení, místní servery, cloudové služby a dokonce Internet věcí. To znamená, že na většinu vašich IT prostředí se mohou vztahovat požadavky obecného nařízení o ochraně osobních údajů.

Splnění požadavků nařízení GDPR nejlépe dosáhnete, pokud se na požadavky nařízení podíváte holisticky a v kontextu všech vašich regulačních a právních závazků týkajících se ochrany osobních údajů. Například mnohá bezpečnostní opatření vyžadovaná nařízením GDPR, jejichž cílem je předcházet hrozbám a narušením bezpečnosti dat, odhalovat je a reagovat na ně, jsou podobná opatřením očekávaným dalšími normami pro ochranu dat, jako je norma ISO 27018 o ochraně osobních údajů v cloudech.

Nejlepším přístupem je identifikace celé sady opatření a možností pro splnění všech požadavků, nikoli sledování opatření vyžadovaných jednotlivými normami nebo předpisy případ od případu. Stejně tak je vhodnější k zajištění souladu s velmi obsažnou regulací jako je GDPR použít komplexní řešení na úrovni platformy zahrnující Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure a Dynamics 365, a nikoli posuzovat jednotlivé technologie a řešení. Takový přístup může přispět nejen k zajištění souladu s GDPR, ale i s dalšími požadavky, které potřebujete plnit nad rámec tohoto nařízení.

Na začátku cesty za splněním požadavků obecného nařízení o ochraně osobních údajů vám doporučujeme zaměřit se na čtyři základní kroky:

- **Mapování –** identifikace osobních údajů, se kterými pracujete, a určení místa jejich uložení
- **Správa –** řízení používání osobních údajů a přístupu k nim
- **Ochrana –** zavedení bezpečnostních opatření, jejichž cílem je předcházet hrozbám a narušením zabezpečení dat, odhalovat je a reagovat na ně
- **Reporting –** vyřizování žádostí o data, ohlašování resp. oznamování případů porušení zabezpečení a udržování požadované dokumentace

Pro každý z těchto kroků uvádíme příklady nástrojů, prostředků a funkcí, které nabízejí různá řešení od společnosti Microsoft a které můžete využít při řešení požadavků příslušného kroku. Přestože tento dokument neposkytuje úplný návod „jak na to“, nabízíme odkazy, které vám pomohou získat podrobnější informace. Další informace najdete také na adrese Microsoft.com/GDPR.

Vzhledem k rozsahu nařízení GDPR byste neměli s přípravou čekat, až toto nařízení vejde v platnost. Je nanejvýš vhodné zkontrolovat postupy ochrany osobních údajů a správy dat už nyní.

V následujících částech jsou popsány konkrétní prvky jednotlivých částí nařízení GDPR a vysvětleny postupy, které můžete použít pro produkty a služby nabízené společností Microsoft již dnes.

Nečekejte a jednejte hned

Mapování: rozpoznání dostupných osobních údajů a určení místa jejich uložení

Jako první krok směřující ke splnění požadavků obecného nařízení o ochraně osobních údajů musíte posoudit, zda se nařízení GDPR vztahuje na vaši organizaci, a pokud ano, tak v jakém rozsahu. K zahájení této analýzy je nutné zjistit, jaká data máte k dispozici a kde jsou uložena.

Vztahuje se nařízení GDPR na moje data?

Obecné nařízení o ochraně osobních údajů reguluje shromažďování, ukládání, používání a sdílení „osobních údajů". Osobní údaje jsou v nařízení GDPR definovány velmi obecně jako *libovolná* data, která se týkají identifikované nebo identifikovatelné fyzické osoby.

Pokud vaše organizace disponuje takovými daty – v databázích zákazníků, ve formulářích zpětné vazby vyplněných zákazníky, v obsahu e-mailů, na fotografiích, v záznamech pořízených systémy CCTV, v záznamech věrnostních programů, v databázích HR nebo kdekoli jinde – nebo je chce shromažďovat a pokud tato data patří obyvatelům EU nebo se jich týkají, pak musíte splnit požadavky nařízení GDPR. Uvědomte si, že nařízení GDPR se vztahuje i na určité osobní údaje, které jsou uložené mimo EU, neboť toto nařízení se týká i dat shromažďovaných, zpracovávaných nebo ukládaných mimo EU, pokud jsou úzce svázána s obyvateli EU.

Vytvoření soupisu

Ke správnému pochopení, zda se obecné nařízení o ochraně osobních údajů *vztahuje* na vaši organizaci, a pokud ano, tak jaké povinnosti z něj vyplývají, je důležité vytvořit soupis dat, která má vaše organizace k dispozici. To vám pomůže rozpoznat, která data jsou osobní, zjistit, v kterých systémech jsou tato data shromažďována a ukládána, a pochopit, proč jsou shromažďována, jak jsou zpracovávána a sdílena a jak dlouho jsou uchovávána.

Zde uvádíme příklady konkrétních způsobů, jak vám naše cloudové a místní nabídky mohou pomoci s prvním krokem nařízení GDPR.

Azure

Vzhledem k tomu, že je Azure otevřená a flexibilní cloudová platforma, zahrnuje službu, která usnadňuje mapování a rozpoznávání zdrojů dat. Microsoft Azure Data Catalog je plně spravovaná cloudová služba, která slouží jako systém registrace a mapování pro zdroje dat vaší organizace. Služba Azure Data Catalog vám tak pomůže mapovat a pochopit zdroje dat a používat je způsobem, který vám umožní získat větší hodnotu ze stávajících dat. Po registraci zdroje dat službou Azure Data Catalog proběhne indexace metadat, aby bylo možné snadno vyhledávat potřebná data.

Dynamics 365

Dynamics 365 nabízí několik funkcí pro vytváření přehledů a auditování, které lze používat prostřednictvím řídicích panelů Dynamics 365 pro vytváření sestav a analýzy k identifikaci osobních údajů:

- Součástí Dynamics 365 je Průvodce sestavou, který usnadňuje vytváření sestav bez použití dotazů XML a SQL.
- Řídicí panely v Dynamics 365 poskytují přehled firemních dat – informací s akcemi, které lze zobrazovat v celé organizaci.
- Microsoft Power BI je platforma samoobslužných funkcí business intelligence (BI), kterou můžete používat k mapování, analýze a vizualizaci dat, ke sdílení získaných přehledů a spolupráci na těchto přehledech se spolupracovníky.

Sada Enterprise Mobility + Security (EMS)

Sada Enterprise Mobility + Security obsahuje bezpečnostní technologie založené na identitě, které vám pomohou mapovat, kontrolovat a chránit osobní údaje uchovávané vaší organizací a také odhalovat potenciální slabá místa a narušení zabezpečení dat.

Microsoft Cloud App Security je komplexní služba, která poskytuje dokonalejší přehled, komplexní opatření a vylepšenou ochranu pro vaše data v cloudových aplikacích. Umožní vám získat přehled o cloudových aplikacích používaných ve vaší síti, neboť rozpozná přes 13 000 aplikací ze všech zařízení, posoudit rizika a provádět průběžnou analýzu.

Microsoft Azure Information Protection pomáhá identifikovat vaše citlivá data a místa jejich uložení. Můžete buď vznést dotaz na data, která mají přiřazenu určitou citlivost, nebo inteligentně rozpoznat citlivá data při vytváření souboru nebo e-mailu. Po rozpoznání mohou být data automaticky kategorizována a označena – vše na základě zásad vyžadovaných společností.

Office 365

Můžeme nabídnout několik specifických řešení Office 365 pro identifikaci osobních údajů nebo správu přístupu k osobním údajům:

- Ochrana před únikem informací (DLP) v produktech Office a Office 365 umožňuje identifikovat přes 80 běžných typů citlivých dat, včetně finančních a zdravotních informací a identifikovatelných osobních údajů.
- Vyhledávání obsahu v Centru zabezpečení a dodržování předpisů Office 365 umožňuje vyhledávat v poštovních schránkách, veřejných složkách, skupinách Office 365, pracovním prostoru Microsoft Teams, webech SharePoint Online, umístěních OneDrivu pro firmy a konverzacích Skypu pro firmy.

- Vyhledávání Office 365 eDiscovery lze používat k nalezení textů a metadat v obsahu napříč vašimi prostředky služeb Office 365, jako jsou SharePoint Online, OneDrive pro firmy, Online Skype pro firmy a Exchange Online.
- Platforma Office 365 Advanced eDiscovery, která využívá technologie strojového učení, pomáhá rozpoznat dokumenty odpovídající určitému tématu (například přezkoumání souladu) rychle a přesněji než tradiční vyhledávání založené na klíčových slovech nebo ruční procházení rozsáhlých množství dokumentů. Advanced eDiscovery může výrazně snížit náklady a vyžadované úsilí při identifikaci souvisejících dokumentů a vztahů dat pomocí strojového učení, které systému umožňuje inteligentně prohledávat rozsáhlé sady dat a rychle se zaměřit na to, co je důležité, čímž se zmenší objem dat před jejich prozkoumáním.
- Rozšířené řízení dat pomáhá s využitím analytických informací a poznatků získaných prostřednictvím strojového učení vyhledávat data, která jsou pro vaši organizaci nejdůležitější, kategorizovat je, nastavovat pro ně zásady a provádět akce v rámci správy jejich životního cyklu.

SharePoint

Můžete využívat Vyhledávací službu SharePoint a funkce pro vyhledávání nabízené aplikací ke sledování osobních údajů. K rozpoznávání a vyhledávání citlivého obsahu nabízí SharePoint Server 2016 stejné funkce ochrany před únikem dat jako Office 365.

SQL Server a Azure SQL Database

Jazyk SQL lze používat k vytváření dotazů do databází a k přizpůsobování nástrojů nebo služeb, které mohou pomoci tento požadavek povolit. Vyhledávání pomocí dotazů je plně podporováno, ačkoli úplné protokolování trasování je nutné provádět na úrovni aplikace. Úkol skriptu poskytuje kód pro provádění vlastních funkcí, jako jsou složité dotazy na data, které nejsou dostupné v integrovaných úkolech a transformacích nabízených službami SSIS (SQL Server Integration Services). Úkol skriptu může také zkombinovat funkce do jednoho skriptu, takže není potřebné použít více úkolů a transformací. Tato sada produktů také zahrnuje výkonné funkce business intelligence, které poskytují koncovým uživatelům přístup k přehledům dat.

Windows a Windows Server

K vyhledávání dat přímo ve Windows můžete využít službu Windows Search, která trasuje a vyhledává osobní údaje na místním počítači a veškerých připojených zařízeních, k nimž máte odpovídající přístupová oprávnění. Pokud chcete vylepšit schopnosti služby Windows Search při vyhledávání cílových dat, můžete je přizpůsobit konfigurací Možností indexování v Ovládacích panelech (například indexování obsahu souborů).

Správa: řízení používání osobních údajů a přístupu k nim

Obecné nařízení o ochraně osobních údajů poskytuje subjektům údajů – jednotlivcům, kterých se tyto údaje týkají – větší kontrolu nad zaznamenáváním a používáním jejich osobních údajů. Subjekt údajů může například požadovat, aby s ním organizace sdílela údaje, které se ho týkají, přenesla jeho údaje do jiných služeb, opravila chyby v jeho údajích nebo vyřadila jisté údaje v určitých případech z dalšího zpracování. V některých případech je nutné tyto žádosti předat během pevně stanovených období.

Řízení dat

K uspokojení vašich závazků vůči subjektům údajů se musíte řádně seznámit s typy osobních údajů, které vaše organizace zpracovává, a způsoby a účely jejich zpracování. Prvním krokem k tomuto seznámení je již dříve zmíněný soupis dat. Po vypracovávání soupisu dat je také důležité vytvořit a zavést plán řízení dat. Plán řízení dat umožňuje definovat zásady, role a odpovědnosti pro přístup k osobním údajům, jejich správu a používání a může vám pomoci zajistit, aby vaše postupy manipulace s daty vyhovovaly nařízení GDPR. Plán řízení dat může například poskytnout vaší organizaci jistotu, že bude efektivně respektovat požadavky subjektů údajů ohledně odstranění nebo přenosu dat.

Cloudové služby společnosti Microsoft

Cloudové služby společnosti Microsoft jsou vyvíjeny pomocí metodologií Microsoft Privacy-by-Design a Privacy-by-Default, aby podporovaly vaši strategii řízení dat. Když svěříte data produktům Azure, Office 365 nebo Dynamics 365, zůstanete výhradními vlastníky těchto dat: zachováte si svá práva, právní nárok i zájem k datům, která uložíte v těchto službách.

Cloudové služby společnosti Microsoft uplatňují vysoce účinná opatření pro ochranu dat vašich zákazníků před neoprávněným přístupem nebo použitím neoprávněnými osobami, jak je podrobně popsáno v Centru zabezpečení Microsoft. Tato opatření zahrnují omezení přístupu zaměstnanců a subdodavatelů společnosti Microsoft a pečlivé vymezení požadavků pro reakci na žádosti orgánů státní správy o data zákazníků.

K údajům vašich vlastních zákazníků však můžete přistupovat kdykoli a z jakéhokoli důvodu.

Kromě toho přesměrujeme žádosti orgánů státní správy o vaše data tak, aby byly předány přímo vám, pokud to není zakázáno zákony, a vzneseme námitky u soudu proti případným pokusům orgánů státní správy zakázat zveřejnění takových žádostí.

K zajištění řádné správy cloudových služeb společnosti Microsoft a k poskytování záruky našim zákazníkům jsou cloudové služby minimálně jednou ročně auditovány podle několika globálních standardů ochrany osobních údajů, jako jsou HIPAA a HITECH, CSA Star Registry a některé normy ISO. Příslušné zprávy najdete na adrese https://servicetrust.microsoft.com/Documents/ComplianceReports.

Kromě těchto závazků poskytujeme nezbytnou kontrolu ohledně řízení dat a přístupu jednotlivých osob k jednotlivým datům v rámci vaší organizace.

Azure

Azure Active Directory je řešení správy identit a přístupu v cloudu. Zajišťuje správu identit a řídí přístup k Azure, místním a dalším cloudovým zdrojům, datům a aplikacím. Azure Active Directory Privileged Identity Management vám umožňuje přiřazovat dočasná práva správce za běhu (JIT) oprávněným uživatelům, aby mohli spravovat prostředky Azure.

Řízení přístupu na základě rolí (Azure RBAC, Role-Based Access Control) vám pomůže řídit přístup k vašim prostředkům Azure. Umožní vám udělovat přístup na základě přiřazené role uživatele, a tím vám usnadní udělování pouze vyžadovaných oprávnění, která uživatelé potřebují k provedení své práce. RBAC můžete přizpůsobit obchodnímu modelu a toleranci rizika vaší organizace.

Office 365

Součástí řešení Office 365 je několik funkcí, které pomáhají se správou osobních údajů:

- Funkce pro řízení dat v Centru zabezpečení a dodržování předpisů Office 365 pomáhají archivovat a uchovávat obsah v poštovních schránkách Exchange Online, na webech SharePointu Online a v umístěních OneDrivu pro firmy a také importovat data do organizace Office 365.
- Funkce Uchovávání ve službách Office 365 pomáhá řídit životní cyklus e-mailů a dokumentů tak, že uchovává potřebný obsah a odstraňuje ten, který už není zapotřebí.
- Rozšířené řízení dat pomáhá s využitím analytických informací a poznatků získaných prostřednictvím strojového učení vyhledávat data, která jsou pro vaši organizaci nejdůležitější, kategorizovat je, nastavovat pro ně zásady a provádět akce v rámci správy jejich životního cyklu.
- Zásady správy informací v SharePointu Online umožňují řídit, jak dlouho se má obsah uchovávat, prostřednictvím auditování sledovat, co lidé s obsahem dělají, a přidávat k dokumentům čárové kódy nebo popisky.
- Zaznamenávání deníku (tzv. žurnál) ve službě Exchange Online pomáhá zajišťovat soulad se zákony, nařízeními a předpisy v organizaci tak, že zaznamenává příchozí a odchozí e-mailovou komunikaci.

Kategorizace dat

Kategorizace dat je důležitou součástí každého plánu řízení dat. Zavedení schématu kategorizace s platností v celé organizaci může být obzvláště užitečné, když budete reagovat na žádosti od subjektů údajů, protože umožňuje snáze identifikovat osobní údaje a zpracovat žádosti, které se těchto údajů týkají.

Dnes nabízíme pokyny a nástroje, které pomáhají vypořádat se se složitostí kategorizace dat.

Azure

Informační brožura Kategorizace dat poskytuje specifické pokyny pro kategorizaci dat v Azure a provede vás technikami, procesem, terminologií a implementací kategorizace dat. Dokumentace obsahuje také celou řadu dalších informací a odkazů.

Dynamics 365

Průvodce plánováním zabezpečení a dodržování předpisů pro Dynamics 365 (online) přináší ucelené pokyny, které vysvětlují klíčové otázky v oblasti dodržování předpisů a zabezpečení, na něž je nutné se zaměřit při plánování nasazení Dynamics 365 (online) v prostředích, jejichž součástí jsou služby integrace podnikového adresáře, jako je synchronizace adresáře a jednotné přihlašování. Nabízí také informace pro zásady ochrany a zajištění důvěrnosti osobních údajů, kategorizaci dat a dopady.

Enterprise Mobility + Security (EMS)

Řešení Azure Information Protection pomáhá kategorizovat a označovat data při jejich vytváření nebo úpravách. Pro citlivá data je pak možné použít ochranu (šifrování plus ověřování plus práva na používání) nebo vizuální označení. Kategorizační popisky a ochrana jsou trvalé a fungují všude, kam se data dostanou, a proto je možné je nepřetržitě identifikovat a chránit bez ohledu na to, kam je uložíte nebo s kým je sdílíte.

Office a Office 365

- Ochrana před únikem informací v produktech Office a Office 365 umožňuje identifikovat více než 80 běžných typů citlivých dat, včetně finančních a zdravotních informací a identifikovatelných osobních údajů. Ochrana před únikem informací navíc organizacím umožňuje nakonfigurovat, jaké akce se mají po nalezení citlivých informací provést, aby byla zajištěna jejich ochrana a předešlo se jejich nechtěnému vyzrazení.

- Rozšířené řízení dat pomáhá s využitím inteligence a poznatků získaných prostřednictvím strojového učení vyhledávat data, která jsou pro vaši organizaci nejdůležitější, kategorizovat je, nastavovat pro ně zásady a provádět akce v rámci správy jejich životního cyklu. Data můžete kategorizovat na základě automatické analýzy a doporučených zásad a následně provádět akce, které zachovají data na místě anebo je naopak odstraní, pokud už nejsou zapotřebí. Office 365 umožňuje zpracovávat místní data i data z externích zdrojů a kategorizovat je podle typu zprávy. Kategorizace typu zprávy umožňuje vyhledávat, uspořádat a exportovat různé zdroje dat, což usnadňuje kontroly v rámci e-discovery.

Windows a Windows Server

Sada Microsoft Data Classification Toolkit pro Windows Server 2012 R2 nabízí příklady výrazů vyhledávání a pravidel, které IT specialistům, auditorům, účetním, právníkům a dalším specialistům na dodržování předpisů ve vaší organizaci pomáhají při provádění aktivit zaměřených na zajištění souladu s předpisy.

Ochrana: Zavedení bezpečnostních opatření, která umožňují předcházet hrozbám a narušením zabezpečení dat, odhalovat je a reagovat na ně

Organizace si stále častěji uvědomují důležitost zabezpečení informací, ale obecné nařízení o ochraně osobních údajů (GDPR) laťku ještě zvyšuje. Vyžaduje, aby organizace přijaly technická a organizační opatření na ochranu osobních údajů před ztrátou, neoprávněným přístupem nebo vyzrazením.

Ochrana vašich dat

Zabezpečení dat není jednoduché. Je potřeba identifikovat a zvážit mnoho typů rizik – od fyzického vniknutí nebo nepoctivých zaměstnanců až po náhodnou ztrátu nebo hackery. Když chcete zajistit dodržování předpisů, je vhodné vytvořit plány řízení rizik a provést kroky k jejich zmírnění, jako je ochrana hesel, auditní logy nebo šifrování.

Cloud společnosti Microsoft je cíleně navržený tak, aby vám pomohl pochopit rizika a chránit se před nimi, a v mnoha směrech je bezpečnější než místní výpočetní prostředí. Naše datacentra mají například certifikaci podle mezinárodně uznávaných bezpečnostních standardů, jsou nepřetržitě fyzicky střežena a přístup k nim podléhá přísným pravidlům.

Ochrana naší cloudové infrastruktury tvoří ale jen část našeho uceleného řešení zabezpečení a každý z našich produktů, ať už v cloudu, nebo v místním prostředí, obsahuje funkce zabezpečení, které vám pomáhají zabezpečit vaše data.

Azure

Následující služby a nástroje Azure vám pomohou ochránit osobní údaje ve vašem cloudovém prostředí:

- Služba Azure Security Center vám poskytuje přehled a umožňuje vám řídit zabezpečení vašich prostředků Azure. Nepřetržitě monitoruje vaše prostředky a nabízí užitečná doporučení pro zabezpečení. Umožňuje vám definovat zásady pro vaše předplatná Azure a skupiny prostředků na základě požadavků vaší organizace na zabezpečení, typů aplikací, které používáte, a citlivosti vašich dat. Doporučení pro zabezpečení, která jsou založena na zásadách, navíc provedou vlastníky služeb procesem implementace potřebných opatření, jako je aktivace antimalwarové ochrany nebo šifrování disků pro vaše prostředky. Služba Security Center také pomáhá rychle nasadit bezpečnostní služby a zařízení od společnosti Microsoft a jejích partnerů, a ještě víc tak posílit ochranu vašeho cloudového prostředí.

- Šifrování dat v systému Azure zajišťuje zabezpečení vašich uložených i přenášených dat. Pomocí služby Storage Service Encryption můžete například automaticky šifrovat svá data při jejich zápisu do služby Azure Storage. Služba Azure Disk Encryption navíc umožňuje zašifrovat disky s operačním systémem a daty používané virtuálními počítači s Windows a Linuxem. Data jsou chráněna i během jejich přenosu mezi aplikací a systémem Azure, a proto jsou nepřetržitě vysoce zabezpečená.
- Služba Azure Key Vault umožňuje zabezpečit vaše kryptografické klíče, certifikáty a hesla, které pomáhají chránit vaše data. Služba Key Vault používá hardwarové moduly zabezpečení HSM (Hardware Security Module) a je navržena tak, že si uchováte kontrolu nad svými klíči a tím pádem i daty a máte jistotu, že si Microsoft nemůže vaše klíče zobrazit ani je extrahovat. Pomocí logování v systému Azure můžete monitorovat a auditovat používání vašich uložených klíčů a importovat své logy do služby Azure HDInsight nebo vašeho vlastního systému SIEM, kde je můžete dále analyzovat a odhalovat pomocí nich možné hrozby.
- Microsoft Antimalware for Azure Cloud Services and Virtual Machines je bezplatná funkce ochrany v reálném čase, která pomáhá odhalovat a odstraňovat viry, spyware a jiný škodlivý software usilující o krádež dat. Poskytuje konfigurovatelné výstrahy, které vás upozorní, když se známý škodlivý nebo nežádoucí software pokusí nainstalovat nebo spustit ve vašich systémech Azure.

Dynamics 365

Koncepce zabezpečení pro Dynamics 365 vám umožňují zajistit integritu dat a ochránit osobní údaje ve vaší organizaci Dynamics 365. Můžete zkombinovat organizační jednotky, zabezpečení založené na rolích, zabezpečení založené na záznamech a zabezpečení založené na polích a kompletně tak definovat, jaký přístup k informacím budou mít uživatelé ve vaší organizaci Dynamics 365.

- Zabezpečení založené na rolích v Dynamics 365 vám umožňuje seskupit oprávnění a omezit tak, jaké úkoly může určitý uživatel provádět. Jedná se o důležitou možnost, zejména když se mění role, které lidé v organizaci zastávají.
- Zabezpečení založené na záznamech v Dynamics 365 umožňuje omezit přístup ke konkrétním záznamům.
- Zabezpečení na úrovni polí v Dynamics 365 umožňuje omezit přístup ke konkrétním důležitým polím, například k polím, která obsahují identifikovatelné osobní údaje.

Enterprise Mobility + Security (EMS)

Ve většině případů, kdy dojde k narušení zabezpečení dat, získávají útočníci přístup do firemní sítě prostřednictvím slabých, výchozích nebo odcizených přihlašovacích údajů. Náš přístup k zabezpečení začíná tím, že chráníme identity na hranicích vašeho prostředí prostřednictvím podmíněného přístupu založeného na rizicích.

- Služba Azure Active Directory (Azure AD) v řešení Enterprise Mobility + Security pomáhá ochránit vaši organizaci na úrovni přístupu tak, že spravuje a chrání vaše identity, včetně identit s vysokými i nízkými oprávněními. Azure AD poskytuje jednu chráněnou identitu pro přístup k tisícům aplikací. Azure AD Premium poskytuje službu vícefaktorového ověřování MultiFactor Authentication (MFA), což je mechanismus řízení přístupu na základě stavu zařízení, lokality uživatele, identity a rizik přihlášení. Nabízí také komplexní sestavy zabezpečení, audity a výstrahy. Služba Azure AD Privileged Identity Management (PIM) pomáhá nacházet, omezovat a monitorovat privilegované identity a jejich přístup k prostředkům pomocí průvodce, kontrol a výstrah. Díky tomu je možné realizovat scénáře, jako je časově omezený přístup (just in time) a přístup s jen nezbytně nutnými oprávněními pro správu (just enough administration).

Řešení Enterprise Mobility + Security poskytuje dokonalý přehled o aktivitách uživatelů a zařízení a datových aktivitách v místním prostředí i v cloudu a pomáhá ochránit vaše data prostřednictvím silných řídicích mechanismů a vynucování zásad.

- Služba Azure Information Protection pomáhá rozšiřovat kontrolu nad vašimi daty na celý životní cyklus dat – to zahrnuje vytvoření a uložení místně nebo v cloudových službách, interní nebo externí sdílení, monitorování distribuce souborů a v neposlední řadě i reakci na neočekávané aktivity.
- Služba Cloud App Security poskytuje dokonalý přehled a výkonné mechanismy řízení dat pro aplikace v modelu Software jako služba (SaaS) a cloudové aplikace, které vaši zaměstnanci používají. Díky tomu máte kompletní informace o kontextu a můžete začít řídit data s použitím detailně definovaných zásad.
- Služba Microsoft Intune poskytuje z cloudu funkce pro správu mobilních zařízení, správu mobilních aplikací a správu počítačů. Intune vám umožňuje zajistit vašim zaměstnancům přístup k podnikovým aplikacím, datům a prostředkům z prakticky libovolného místa a současně pomáhá zachovat vysokou úroveň zabezpečení podnikových informací.

Office a Office 365

Zabezpečení je nedílnou součástí platformy Office 365 na všech úrovních, od vývoje aplikací, přes fyzická datacentra až po přístup koncových uživatelů. Aplikace Office 365 obsahují integrované funkce zabezpečení, které zjednodušují proces ochrany dat, a současně vám umožňují flexibilně konfigurovat, spravovat a integrovat zabezpečení tak, jak vyžadují vaše jedinečné obchodní potřeby. Rámec Office 365 pro dodržování předpisů má více než 1 000 prvků, díky nimž může Office 365 držet krok s neustále se vyvíjecími standardy v odvětví, které zahrnují více než 50 certifikací a osvědčení.

Celá řada bezpečnostních opatření je dostupná ve výchozím nastavení. Produkty SharePoint i OneDrive pro firmy například používají šifrování přenášených a uložených dat. Navíc můžete nakonfigurovat a nasadit digitální certifikáty, které skrývají osobní údaje. Ovládací prvky přístupu v systému Office vám umožňují udělovat nebo omezovat přístup k osobním údajům.

Office 365 nabízí další funkce, které pomáhají chránit data a odhalovat narušení zabezpečení dat:

- Služba Secure Score informuje o stavu zabezpečení a o tom, pomocí kterých dostupných funkcí můžete snížit rizika a současně dosáhnout rovnováhy mezi produktivitou a zabezpečením.
- Rozšířená ochrana před internetovými útoky pro Exchange Online pomáhá chránit v reálném čase e-mail před novými, rafinovanými útoky malwaru. Umožňuje také vytvářet zásady, které pomáhají zamezit uživatelům v přístupu ke škodlivým přílohám nebo webům, na něž z e-mailu vedou odkazy. Součástí Rozšířené ochrany před internetovými útoky pro Exchange Online je ochrana před neznámým malwarem a viry, ochrana před nebezpečnými adresami URL v okamžiku, kdy na ně uživatel klikne, bohaté možnosti generování sestav a funkce pro sledování adres URL.
- Správa přístupových práv k informacím (IRM) umožňuje vám a vašim uživatelům zabránit tomu, aby si neoprávněné osoby mohly vytisknout, přeposlat, uložit, upravit nebo zkopírovat citlivé informace. Správa přístupových práv k informacím v SharePointu Online umožňuje omezit, jaké akce (například tisk kopií souborů nebo kopírování textu) mohou uživatelé provádět se soubory, které byly staženy ze seznamů nebo knihoven. Správa přístupových práv k informacím ve službě Exchange Online pomáhá zabránit vyzrazení citlivých informací v e-mailových zprávách a přílohách prostřednictvím e-mailu, online i offline.
- Správa mobilních zařízení (MDM) pro Office 365 umožňuje nastavit zásady a pravidla, které pomáhají zabezpečit a spravovat zaregistrovaná zařízení uživatelů, jako jsou iPhony, iPady a zařízení se systémy Android nebo Windows. Můžete například zařízení vzdáleně vymazat nebo procházet sestavy s podrobnými informacemi o zařízeních. Office 365 také poskytuje vyšší úroveň zabezpečení prostřednictvím vícefaktorového ověřování.

SQL Server a Azure SQL Database

SQL Server a Azure SQL Database poskytují mechanismy pro řízení přístupu k databázím a správu oprávnění na několika úrovních:

- Brána firewall služby Azure SQL Database omezuje přístup k jednotlivým databázím na serveru služby Azure SQL Database tak, že přístup povoluje jen prostřednictvím autorizovaných připojení. Můžete vytvářet pravidla brány firewall na úrovni serveru a na úrovni databází a určit rozsah schválených IP adres, ze kterých je možné se připojit.
- Ověřování SQL Serveru pomáhá zajistit, že k databázovému serveru budou mít přístup jen autorizovaní uživatelé s platnými přihlašovacími údaji. SQL Server podporuje ověřování systému Windows i účty pro SQL Server. Ověřování systému Windows nabízí integrované zabezpečení a představuje doporučenou možnost s vyšší úrovní zabezpečení, protože celý proces ověřování je šifrovaný. Azure SQL Database podporuje ověřování prostřednictvím služby Azure Active Directory, které nabízí možnost jednotného přihlašování a je podporované pro spravované a integrované domény.
- Autorizace SQL Serveru umožňuje spravovat oprávnění na základě principu nejnižšího potřebného oprávnění. SQL Server a SQL Database používají zabezpečení založené na rolích, které podporuje odstupňované řízení oprávnění pro data prostřednictvím správy členství v rolích a oprávnění na úrovni objektů.
- Dynamické maskování dat (DDM) je integrovaná funkce, která umožňuje omezit přístup k citlivým datům tak, že data zamaskuje, když k nim přistupují uživatelé nebo aplikace bez potřebných oprávnění. Data v databázi zůstávají nedotčená a jen se dynamicky maskují určená datová pole ve výsledcích dotazů. Dynamické maskování dat je jednoduché nakonfigurovat a nevyžaduje žádné změny v aplikacích. Pro uživatele, kteří používají Azure SQL Database, může dynamické maskování dat automaticky mapovat potenciálně citlivá data a navrhovat, jaké masky je vhodné použít.
- Zabezpečení na úrovni řádků (RLS) je další integrovaná funkce, pomocí níž zákazníci s produkty SQL Server a SQL Database mohou implementovat omezení přístupu k řádkům dat. RLS umožňuje podrobně definovat přístup k řádkům v tabulce databáze a poskytuje tak větší kontrolu nad tím, kteří uživatelé mají přístup ke kterým datům. Logika omezení přístupu se nachází v databázové vrstvě, a proto tato funkce významně zjednodušuje návrh a implementaci zabezpečení aplikací.

SQL Server a SQL Database poskytují sadu výkonných funkcí, které chrání data a umožňují zjistit, zda došlo k narušení zabezpečení dat:

- Transparentní šifrování dat (Transparent data encryption) chrání uložená data tak, že na úrovni fyzického úložiště šifruje soubory databáze, souvisejících záloh a transakčního protokolu. Toto šifrování je pro aplikace transparentní a ke zvýšení výkonu používá hardwarovou akceleraci.
- Protokol TLS (Transport Layer Security) zajišťuje ochranu dat přenášených prostřednictvím připojení ke službě SQL Database.
- Funkce Always Encrypted, která v odvětví zatím nemá obdoby, chrání vysoce citlivá data v produktech SQL Server a SQL Database. Umožňuje klientům šifrovat citlivá data v rámci klientských aplikací a přitom databázovému stroji nikdy nezpřístupňuje šifrovací klíče. Tento mechanismus je pro aplikace transparentní, protože šifrování a dešifrování transparentně zajišťuje klientský ovladač podporující funkci Always Encrypted.
- Auditování pro SQL Database a audit SQL Serveru sledují události databáze a zapisují je do protokolu auditu. Auditování poskytuje přehled o probíhajících aktivitách v databázi a umožňuje také analyzovat a prošetřovat minulé aktivity s cílem odhalit možné hrozby nebo případná zneužití a narušení zabezpečení.
- Detekce hrozeb ve službě SQL Database odhaluje anomálie v databázových aktivitách a upozorňuje tak na hrozby, kterým databáze může případně čelit. S použitím sady pokročilých algoritmů se detekce hrozeb soustavně učí a profiluje chování aplikace a upozorňuje na neobvyklou nebo podezřelou aktivitu ihned po jejím zjištění. Detekce hrozeb vám pomůže plnit požadavek nařízení GDPR na oznamování narušení zabezpečení údajů.

Windows a Windows Server

Součástí systémů Windows 10 a Windows Server 2016 je špičkové šifrování, antimalwarové technologie a řešení pro správu identit a přístupu, která umožňují přejít od hesel na bezpečnější formy ověřování:

- Windows Hello představuje pohodlnou alternativu na podnikové úrovni, která umožňuje ověřovat identity namísto hesel přirozeně (s použitím biometrických údajů) nebo pro uživatele známým způsobem (s použitím kódů PIN) a poskytuje přitom stejné přínosy zabezpečení jako čipové karty bez potřeby dalších periferií.
- Antivirová ochrana v programu Windows Defender je spolehlivé antimalwarové řešení, které vám okamžitě zajistí ochranu. Antivirová ochrana v programu Windows Defender rychle odhaluje nový malware a poskytuje před ním ochranu a může okamžitě ochránit vaše zařízení, když v jakékoli části svého prostředí objevíte nějakou hrozbu.
- Funkce Device Guard vám umožňuje uzamknout vaše zařízení a servery a ochránit je tak před novými a neznámými variantami malwaru a pokročilými trvalými hrozbami. Na rozdíl od řešení založených na detekci, jako jsou antivirové programy, která nedokážou odhalit nejnovější hrozby, pokud je neustále neaktualizujete, ochrana Device Guard vaše zařízení uzamkne, takže mohou spouštět jen vámi vybrané autorizované aplikace. To představuje velmi efektivní způsob, jak se s malwarem vyrovnat.
- Credential Guard je funkce, která izoluje vaše tajné kódy na zařízení, například vaše tokeny pro jednotné přihlašování, takže je není možné zneužít, ani když je zcela překonána ochrana operačního systému Windows. Toto řešení v podstatě znemožňuje útoky, před kterými se lze jinak jen těžko bránit, jako jsou útoky typu Pass the Hash.
- Nástroj BitLocker Drive Encryption v systémech Windows 10 a Windows Server 2016 poskytuje šifrování na podnikové úrovni, které pomáhá ochránit vaše data, pokud dojde ke ztrátě nebo odcizení vašeho zařízení. BitLocker plně šifruje disk a přenosné paměti flash v počítači, a znemožňuje tak neoprávněným uživatelům přístup k datům.
- Funkce Windows Information Protection navazuje tam, kde končí možnosti nástroje BitLocker. Zatímco nástroj BitLocker chrání celý disk nebo zařízení, Windows Information Protection chrání vaše data před neoprávněnými uživateli a spuštěnými aplikacemi v počítači. Pomáhá také předcházet tomu, aby se údaje dostaly z firemních do jiných dokumentů nebo na web.
- Chráněné virtuální počítače šifrují pomocí nástroje BitLocker disky a virtuální počítače, které používají technologii Hyper-V. K obsahu chráněných virtuálních počítačů tak nebudou mít přístup ani správci, pokud by chtěli zneužít svých pravomocí nebo pokud by došlo k vyzrazení jejich přihlašovacích údajů.

- Technologie Just Enough Administration a Just in Time Administration umožňují správcům provádět potřebné úkony, ale současně máte možnost určit, v jakém rozsahu a čase mohou správci tyto úkoly plnit. Výrazně se tak omezí rozsah škod v případě, že dojde ke zneužití přihlašovacích údajů se zvýšenými oprávněními. Tyto technologie poskytují správcům jen takovou úroveň přístupu, jakou potřebují, a jen v době, kdy pracují na určitém projektu.

Odhalování narušení zabezpečení dat a reakce na ně

Obecné nařízení o ochraně osobních údajů (GDPR) v některých případech vyžaduje, aby organizace urychleně uvědomily příslušné úřady, když dojde k narušení zabezpečení dat. V některých případech musejí organizace uvědomit také subjekty údajů, kterých se incident týká. Při plnění tohoto požadavku je pro organizace přínosné, když mohou monitorovat a odhalovat vniknutí do systému.

Pro incidenty, u kterých je reakce částečně nebo zcela naší odpovědností, jsme zavedli procesy Security Incident Response Management (Řízení reakce na incidenty zabezpečení), které jsou popsány pro Azure a Office 365.

Kromě toho definujeme, jak spolupracujeme se zákazníky v rámci modelu sdílené odpovědnosti, který je popsán v informační brožuře Sdílené odpovědnosti v cloud computingu.

Když zjistíte možné narušení zabezpečení, doporučujeme vám použít následující proces sestávající ze čtyř kroků, který používáme i v našem vlastním programu reakce na incidenty:

- Vyhodnoťte dopady a závažnost události. V závislosti na zjištěných skutečnostech může nebo nemusí dojít k eskalaci na reakční tým kybernetického zabezpečení / ochrany dat.
- Proveďte technické nebo forenzní šetření a určete strategie pro zamezení šíření, omezení dopadu a alternativní řešení. Pokud se tým kybernetického zabezpečení / ochrany dat domnívá, že mohlo dojít k vyzrazení osobních údajů osobě, která jedná protiprávně nebo nemá pro přístup k těmto údajům oprávnění, je souběžně zahájen oznamovací proces, jak vyžaduje nařízení GDPR.
- Vytvořte plán obnovy pro zmírnění dopadů. Souběžně s diagnostikou je nutné okamžitě provést krizové kroky pro zamezení šíření problému, například umístit postižené systémy do karantény. Je možné naplánovat dlouhodobé kroky nápravy, které realizujete, až pomine bezprostřední riziko.
- Vytvořte následnou analytickou zprávu, která uvádí podrobnosti incidentu a jejímž cílem je revidovat zásady, procesy a postupy, aby se událost nemohla opakovat. Tato fáze odpovídá článku 31 nařízení GDPR, který požaduje zaznamenat fakta spojená s narušením zabezpečení, jeho dopady a přijatá nápravná opatření.

Azure

Chránit osobní údaje ve vašich systémech a oznamovat a kontrolovat stav dodržování předpisů patří mezi hlavní požadavky nařízení o ochraně osobních údajů (GDPR). S plněním těchto závazků, které vyplývají z nařízení GDPR, vám pomohou následující služby a nástroje Azure:

- Služby integrované s Azure vám umožňují rychle a snadno zjišťovat celkový stav zabezpečení a také odhalovat a prošetřovat hrozby ve vašem cloudovém prostředí. Služba Azure Security Center využívá pokročilou analýzu zabezpečení. Převratné technologie v oblasti velkých objemů dat a strojového učení umožňují vyhodnocovat události v celé cloudové infrastruktuře – odhalovat hrozby a předvídat vývoj útoků by s použitím ručně prováděných postupů bylo nemožné. Součástí této analýzy zabezpečení je:

    - Integrovaná analýza hrozeb, která vyhledává známé nežádoucí aktivity s využitím globálních znalostí hrozeb z produktů a služeb Microsoftu, oddělení Microsoft Digital Crimes Unit (DCU), služby Microsoft Security Response Center (MSRC) a externích informačních zdrojů

    - Behaviorální analýza, která na základě známých vzorců odhaluje škodlivé chování

    - Detekce anomálií, která s využitím statistického profilování porovnává současné a minulé chování. Upozorňuje na odchylky od zjištěného výchozího stavu, které odpovídají vektoru možného útoku.

  Služba Security Center navíc poskytuje prioritní výstrahy zabezpečení, které umožňují pochopit, jak útok probíhá, včetně souvisejících událostí a zasažených prostředků.

    - Služba Azure Log Analytics nabízí konfigurovatelné možnosti auditování a protokolování zabezpečení, které pomáhají shromažďovat a analyzovat data generovaná prostředky ve vašem cloudovém nebo místním prostředí. S využitím integrovaného hledání a přizpůsobených řídicích panelů přináší poznatky v reálném čase a umožňuje tak okamžitě analyzovat milióny záznamů ze všech aplikačních úloh a serverů bez ohledu na jejich fyzické umístění. Podporuje rychlou reakci a důkladné prošetření jakýchkoli událostí souvisejících se zabezpečením.

Dynamics 365

Řešení Dynamics 365 (online) pravidelně udržujeme a aktualizujeme, abychom zajistili jeho zabezpečení, výkon a dostupnost a zpřístupnili nové funkce. Čas od času také reagujeme na incidenty ve službách. O všech těchto aktivitách dostává e-mailem oznámení uživatel, který je pro vaši organizaci správcem Dynamics 365. Během incidentu, který má dopad na poskytování služby, vás může zástupce oddělení služeb zákazníkům pro Dynamics 365 (online) také kontaktovat telefonicky nebo informace doplnit v e-mailu. Veškeré podrobnosti o našich zásadách a sděleních pro Dynamics 365 najdete na webu TechNet.

Enterprise Mobility + Security (EMS)

Naše komplexní analýza hrozeb využívá špičkové technologie behaviorální analýzy a detekce anomálií, které umožňují odhalovat podezřelé aktivity a zjišťovat hrozby v místním prostředí i v cloudu. To zahrnuje známé útoky (například typu Pass the Hash nebo Pass the Ticket) a chyby zabezpečení ve vašem systému. Na odhalené hrozby můžete okamžitě reagovat a obnovit normální stav s využitím výkonných prostředků podpory. Naši analýzu hrozeb ještě dále vylepšuje graf inteligentního zabezpečení Microsoft, který využívá rozsáhlé datové sady a strojové učení v cloudu:

- Microsoft Advanced Threat Analytics (ATA) je produkt pro místní nasazení, který IT specialistům na zabezpečení pomáhá chránit jejich organizace před pokročilými cílenými útoky tím, že automaticky analyzuje, učí se a rozpoznává normální a abnormální chování entit (uživatelů, zařízení a prostředků). Řešení ATA odhaluje pokročilá trvalá ohrožení v místním prostředí díky tomu, detekuje podezřelé chování uživatelů a entit (zařízení a prostředků) s využitím strojového učení a informací v místní službě Active Directory, systémech SIEM a protokolech systému Windows. Odhaluje také známé útoky (například typu Pass the Hash). V neposlední řadě poskytuje jednoduchou časovou osu útoku a jasné, relevantní informace o útoku, které umožňují rychle se zaměřit na to, co je důležité.
- Služba Cloud App Security zajišťuje pro vaše cloudové aplikace ochranu před hrozbami na základě rozsáhlých znalostí, které společnost Microsoft shromáždila, a výzkumu, který hrozbám věnuje. Umožní vám předcházet hrozbám tím, že odhaluje používání vysoce rizikových aplikací, bezpečnostní incidenty a neobvyklé chování uživatelů. S použitím pokročilých heuristických algoritmů strojového učení se řešení Cloud App Security učí, jak uživatelé s jednotlivými aplikacemi SaaS pracují, a na základě behaviorální analýzy vyhodnocuje riziko každé transakce. To zahrnuje souběžné přihlášení ze dvou různých zemí, nenadálé stažení terabajtů dat nebo několik nezdařených pokusů o obnovení zapomenutého hesla, které mohou signalizovat útok hrubou silou.
- Služba Azure Active Directory (Azure AD) Premium odhaluje hrozby v cloudu na úrovni identit. Monitoruje používání aplikací a chrání vaši firmu před pokročilými hrozbami na základě generování sestav a monitorování zabezpečení. Sestavy s informacemi o přístupu a používání poskytují přehled o stavu a zabezpečení adresáře vaší organizace. Služba Azure AD navíc chrání identity prostřednictvím oznámení, analýzy a doporučených kroků nápravy.

Office a Office 365

Office 365 nabízí několik funkcí, které pomáhají odhalovat narušení zabezpečení dat a reagovat na ně:

- Analýza hrozeb (Threat Intelligence) pomáhá proaktivně odhalovat pokročilé hrozby ve službách Office 365 a zajistit před nimi ochranu. Rozsáhlé znalosti hrozeb, které dokážeme shromáždit díky globální působnosti Microsoftu, grafu inteligentního zabezpečení a podnětům od specialistů na boj s kybernetickými hrozbami, pomáhají rychle a efektivně nastavit výstrahy, dynamické zásady a řešení zabezpečení.
- Rozšířená správa zabezpečení (Advanced Security Management) umožňuje odhalovat vysoce rizikové a abnormální používání, které může svědčit o narušení zabezpečení. Navíc umožňuje nastavit zásady pro aktivity a prostřednictvím nich sledovat rizikové akce a podezřelé aktivity a následně na ně reagovat. Funkce Productivity App Discovery pro mapování kancelářských aplikací vám navíc prostřednictvím informací z protokolů vaší organizace poskytuje přehled o tom, jaké aplikace Office 365 a další cloudové aplikace vaši uživatelé používají, a na základě těchto poznatků provádět patřičné kroky.
- Rozšířená ochrana před internetovými útoky (Advanced Threat Protection) pro Exchange Online pomáhá chránit v reálném čase e-mail před novými, rafinovanými útoky malwaru. Umožňuje také vytvářet zásady, které pomáhají zamezit uživatelům v přístupu ke škodlivým přílohám nebo webům, na něž z e-mailu vedou odkazy.

SQL Server a Azure SQL Database

Produkty SQL Server a SQL Database poskytují sadu výkonných integrovaných funkcí, které umožňují zjistit, zda došlo k narušení zabezpečení dat:

- Auditování pro SQL Database a audit SQL Serveru sledují události databáze a zapisují je do protokolu auditu. Auditování poskytuje přehled o probíhajících aktivitách v databázi a umožňuje také analyzovat a prošetřovat minulé aktivity s cílem odhalit možné hrozby nebo případná zneužití a narušení zabezpečení.
- Detekce hrozeb (Threat Detection) ve službě SQL Database odhaluje anomálie v databázových aktivitách a upozorňuje tak na hrozby, kterým databáze může případně čelit. S použitím sady pokročilých algoritmů se detekce hrozeb soustavně učí a profiluje chování aplikace a upozorňuje na neobvyklou nebo podezřelou aktivitu ihned po jejím zjištění. Detekce hrozeb vám pomůže plnit požadavek nařízení GDPR na oznamování narušení zabezpečení údajů.

Windows a Windows Server

Rozšířená ochrana před internetovými útoky v programu Windows Defender (Windows Defender Advanced Threat Protection, ATP) umožňuje provoznímu týmu, který zodpovídá za zabezpečení, odhalovat narušení zabezpečení dat ve vaší síti, prošetřovat je, omezovat jejich dopad a provádět nápravná opatření. Toto řešení poskytuje pokročilé funkce pro detekci narušení zabezpečení, jejich prošetřování a nápravu, které pokrývají všechny koncové body a mají k dispozici historická data za dobu až 6 měsíců, a to dokonce i když jsou koncové body offline, mimo síťovou doménu, došlo k jejich obnovení s použitím bitové kopie nebo už neexistují. Rozšířená ochrana před internetovými útoky v programu Windows Defender pomáhá plnit klíčový požadavek nařízení GDPR, a sice mít jasné postupy pro odhalování narušení zabezpečení dat, jejich prošetřování a oznamování.

Reporting: vyřizování žádostí o data, oznamování narušení zabezpečení dat a udržování požadované dokumentace

Obecné nařízení o ochraně osobních údajů vytyčuje nové standardy, co se týče transparentnosti, odpovědnosti a uchovávání záznamů. Vyžaduje od vás větší transparentnost nejen v tom, jak zpracováváte osobní údaje, ale také v tom, jak aktivně udržujete dokumentaci, která definuje vaše procesy a používání osobních údajů.

Uchovávání záznamů

Organizace zpracovávající osobní údaje budou muset uchovávat záznamy, které poskytují následující informace: účely zpracování; kategorie zpracovávaných osobních údajů; identity třetích stran, s nimiž jsou údaje sdíleny; zda byly osobní údaje přeneseny do třetích zemí (a kterých); právní základ takových přenosů; organizační a technická bezpečnostní opatření a doba uchovávání údajů platná pro různé sady dat. Jednou z možností, jak toho dosáhnout, je používat auditovací nástroje, které zajišťují, že je sledováno a zaznamenáváno jakékoli zpracování údajů, ať už jejich shromažďování, používání, sdílení, nebo jiná manipulace s nimi.

Cloudové služby Microsoft nabízejí integrované auditovací služby, které pomáhají zajistit dodržování tohoto standardu.

Azure, Office 365 a Dynamics 365

Na portálu Service Trust Portal najdete ucelené informace o různých nabídkách pro zajištění souladu s předpisy, zabezpečení, ochranu osobních údajů a zachování důvěryhodnosti ve službách Azure, Office 365 a Dynamics 365, včetně zpráv a osvědčení. Díky nezávislým auditům a vyhodnocením v oblasti GRC (Governance, Risk management, Compliance – dohled, řízení rizik a dodržování předpisů) máte neustálý přehled o tom, jak cloudové služby Microsoft plní globální standardy, které jsou pro vaši organizaci důležité. Dokumentace dokládající důvěryhodnost vám pomáhá pochopit, jak cloudové služby Microsoft chrání vaše data a jak ve svých cloudových službách můžete řídit zabezpečení dat a dodržování předpisů.

Azure

Auditování a protokolování událostí a výstrah souvisejících se zabezpečením patří mezi důležité součásti efektivní strategie ochrany dat.

Funkce Azure pro protokolování a auditování vám umožňují:

- Vytvářet záznamy pro auditování aplikací nasazených v Azure a virtuálních počítačů vytvořených z galerie virtuálních počítačů Azure
- Centrálně analyzovat velké sady dat na základě shromažďování událostí zabezpečení z řešení Azure IaaS (infrastruktura jako služba) a PaaS (platforma jako služba). Služba

Azure HDInsight vám pak umožní tyto události agregovat a analyzovat nebo je můžete exportovat do místních systémů SIEM, které zajišťují soustavné monitorování.

- Monitorovat sestavy s informacemi o přístupu a používání s využitím protokolování administrativních operací, které Azure nabízí, včetně přístupu k systému, a vytvářet tak záznamy pro audit pro případ neoprávněných nebo nechtěných změn. Můžete načítat protokoly auditování pro svého tenanta služby Azure Active Directory a procházet sestavy s informacemi o přístupu a používání.
- Exportovat výstrahy zabezpečení do místních systémů SIEM s použitím služby Azure Diagnostics, kterou je možné nakonfigurovat tak, aby shromažďovala protokoly událostí zabezpečení systému Windows a další protokoly související se zabezpečením
- Na webu Azure Marketplace získat nástroje od třetích stran pro monitorování zabezpečení, vykazování a zasílání výstrah

Služba Microsoft Azure Monitor umožňuje organizacím zobrazit si a spravovat všechny úkoly monitorování dat na jednom centrálním řídicím panelu. Získáte podrobné aktuální údaje o výkonu a využití dat, a přístup k protokolům aktivit, které sledují každé volání rozhraní API, spolu s diagnostickými protokoly, které pomáhají sledovat problémy s prostředky Azure. Navíc máte možnost nastavovat výstrahy a provádět automatizované akce. Služba Azure Monitor podporuje integraci s vašimi stávajícími nástroji. Když spojíte Azure Monitor s analytickými nástroji, které už dobře znáte, získáte tak ucelené řešení monitorování s bohatou sadou funkcí.

Office a Office 365

- V části Zajištění služeb v Centru zabezpečení a dodržování předpisů Office 365 najdete podrobné informace pro vyhodnocení rizik, včetně podrobných zpráv o dodržování předpisů společností Microsoft a transparentních informací o stavu auditovaných řídicích mechanismů. Tyto informace zahrnují:
- Postupy, které Microsoft používá pro zabezpečení zákaznických dat uložených v Office 365
- Zprávy z nezávislých auditů služeb Office 365
- Podrobnosti o implementaci a testování kontrolních mechanismů pro zabezpečení, ochranu osobních údajů a dodržování předpisů, které zákazníkům pomáhají plnit standardy, zákony a nařízení v různých odvětvích, jako jsou normy ISO 27001 a ISO 27018 nebo zákon HIPAA (Health Insurance Portability and Accountability Act)

- Protokoly auditu Office 365 umožňují monitorovat a sledovat aktivity uživatelů a správců pro všechny aplikační úlohy Office 365, což pomáhá včas odhalovat a prošetřovat problémy se zabezpečením a dodržováním předpisů. Na stránce vyhledávání v protokolu auditu Office 365 můžete začít zaznamenávat činnosti uživatelů a správců ve vaší organizaci. Až Office 365 připraví protokol auditu, můžete v něm vyhledávat nejrůznější aktivity, včetně ukládání na OneDrive nebo SharePoint Online a resetování hesel uživatelů. Pro Exchange Online je možné nastavit sledování změn prováděných správci a sledovat všechny případy, kdy k poštovním schránkám přistupuje někdo jiný než vlastník schránky.
- Customer Lockbox vám umožňuje řídit, jak mohou specialisté podpory Microsoftu přistupovat k vašim datům, když vám budou poskytovat pomoc. Pokud diagnostika a řešení problému vyžaduje, aby měl specialista k vašim datům přístup, Customer Lockbox vám umožňuje povolit nebo zamítnout žádost o přístup. Pokud ji schválíte, bude mít specialista k datům přístup. Každá žádost má dobu platnosti a po vyřešení je žádost uzavřena a oprávnění k přístupu odvoláno.

Enterprise Mobility + Security (EMS)

Služba Azure Information Protection nabízí bohaté funkce pro protokolování a generování sestav, které umožňují analyzovat, jak jsou distribuována citlivá data. Sledování dokumentů umožňuje uživatelům a správcům monitorovat aktivity prováděné se sdílenými daty a odvolat přístup, pokud se vyskytnou neočekávané události. Služba Azure Information Protection také poskytuje funkce pro analýzu nestrukturovaných dat, která se nacházejí ve sdílených složkách, na webech a v knihovnách SharePointu, online úložištích a jednotkách stolních nebo přenosných počítačů. Díky přístupu k souborům můžete kontrolovat obsah každého souboru a zjišťovat, jestli obsahuje určité kategorie osobních údajů. Každý soubor pak můžete kategorizovat a přidat k němu popisek podle toho, jaká data se v něm vyskytují. Pro tento proces navíc můžete generovat sestavy s informacemi o tom, které soubory byly zkontrolovány, jakým kategorizačním zásadám vyhovovaly a jaký popisek byl pro ně použit.

Windows a Windows Server

Protokol událostí systému Windows nabízí široké možnosti protokolování, které správcům umožňují prohlížet si zaznamenané informace o aktivitách operačního systému, aplikací a uživatelů. Tento systém protokolování je možné nakonfigurovat tak, aby podrobně auditoval akce uživatelů a aplikací, včetně přístupu k souborům, používání aplikací nebo změn zásad. Protokol událostí systému Windows také správcům umožňuje přeposílat události z klientských počítačů a serverů do centrálního umístění pro účely vykazování a auditování.

Nástroje pro vykazování a dokumentace cloudových služeb

Stejně jako u jakékoli jiné databáze nebo systému, který nakládá s osobními údaji, by vaše organizace měla dobře zaznamenat a chápat, jak cloudové služby používáte. Vaše organizace například musí mít přehled o tom, jaké osobní údaje vaším jménem uchovávají poskytovatelé služeb, jaké smlouvy upravují vztahy s těmito poskytovali služeb a co se s daty stane, když vám váš partner přestane službu poskytovat.

Se správou těchto informací vám pomáháme tím, že udržujeme jednoduché a srozumitelné vykazovací nástroje pro váš účet v cloudu od společnosti Microsoft spolu s rozsáhlou dokumentací o našich cloudových službách, o tom, jak fungují, a o našem smluvním vztahu s vámi.

Informování subjektů údajů

Nařízení GDPR změní požadavky na ochranu osobních údajů a zpřísní povinnosti zpracovatelů a správců údajů, co se týče oznamování narušení zabezpečení osobních údajů, která vedou k ohrožení práv a svobod občanů. Podle tohoto nového nařízení, tak jak definují články 17, 31 a 32, musí zpracovatel o každém takovém narušení zabezpečení osobních údajů neprodleně informovat, jakmile se o něm dozví.

Po zjištění narušení zabezpečení musí správce údajů informovat příslušný úřad pověřený ochranou údajů do 72 hodin. Pokud je pravděpodobné, že takové narušení bude mít za následek vysoké riziko pro práva a svobody jednotlivců, budou správci také muset bez zbytečného odkladu oznámit tuto skutečnost postiženým jednotlivcům. Pokud ve své roli správce údajů používáte zpracovatele údajů, musíte mít tedy jistotu, že smlouvy jasně definují, co se pro oznamování případných narušení zabezpečení od vašich smluvních partnerů očekává.

Pro incidenty, u kterých je reakce částečně nebo zcela odpovědností společnosti Microsoft, jsme zavedli procesy Security Incident Response Management (Řízení reakce na incidenty zabezpečení), které jsou popsány pro Azure, Office 365 a Dynamics 365. Naše závazky v souvislosti s nařízením GDPR také definujeme v našich smlouvách.

Pro produkty a služby Microsoft, například Azure, Dynamics 365, Enterprise Mobility + Security, Office 365 nebo Windows 10, jsou v současnosti dostupná řešení, která pomáhají odhalovat a vyhodnocovat hrozby a narušení zabezpečení a plnit závazky vyplývající pro jejich oznamování z nařízení GDPR.

Vyřizování žádostí od subjektů údajů

Mezi nejvýznamnější prvky nařízení GDPR patří práva subjektů údajů, která jsou v článcích tohoto nařízení stanovena v oddílu 2: Informace a přístup k osobním údajům, v oddílu 3: Oprava a výmaz a v oddílu 4: Právo vznést námitku a automatizované individuální rozhodování.

Tyto závazky mohou mít dopad na vaše prostředí a provoz IT jakožto správce údajů a také na prostředí a provoz IT jakéhokoli poskytovatele služeb, kterého angažujete jako zpracovatele údajů.

Řádné řízení dat je klíčovou součástí zákonů na ochranu osobních údajů a prosazuje ho většina zákonů a nařízení na ochranu dat a osobních údajů. Mezi klíčové prvky řízení podle nařízení GDPR patří pověřenec pro ochranu osobních údajů, kterého je nutné jmenovat za okolností uvedených v článcích 35, 36 a 37. Pověřenec pro ochranu osobních údajů musí být zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.

Dalším důležitým prvkem řízení podle nařízení GDPR je zpracování tzv. posouzení vlivu na ochranu osobních údajů pod vedením pověřence pro ochranu osobních údajů. Článek 33a konkrétně uvádí požadavky, podle kterých musí správce údajů do dvou let od vyhotovení posouzení vlivu na ochranu osobních údajů provést kontrolu dodržování a doložit, že zpracování osobních údajů probíhá v souladu s posouzením vlivu na ochranu osobních údajů. Článek 35-*11: Pokud je to nutné, správce musí prověřit, zda zpracování probíhá v souladu s vyhodnocením dopadu ochrany dat minimálně v případě, kdy dochází ke změně rizika vyplývajícího z operací zpracování.*

Centrum zabezpečení Microsoft poskytuje informace o tom, jak vás můžeme ve vaší činnosti podporovat. K dispozici je mimo jiné speciální oddíl věnovaný názorům a závazkům Microsoftu v souvislosti s nařízením GDPR.