Bádensko-Wiirttembersko

1JER LAI\OES POŽADAVKY NA OCHRANU ÚDAJŮ **LM> CS** t\FREE OF INFORMATION

Pilotní využití MS ve školách: doporučení LfDI

Hodnocení a doporučení z monitorování pilotního projektu *Možné zavedení Microsoft (Office 365) jako* Saas *v rámci platformy digitálního vzdělávání"* Ministerstva kultury, mládeže a sportu státním komisařem pro ochranu dat a svobodu informací Bádenska-Württemberska.

Ref. 6510-1/2 Stuttgart, 23. dubna 2021

Obsah

1Popis pilotního projektu a Doporučení

Státní komisař pro ochranu údajů a svobodu informací Bádenska-Württemberska (LfDI) se jako poradce podílel na pilotním projektu ministerstva školství, mládeže a sportu Bádenska-Württemberska týkajícím se používání verze Microsoft Office 365 (f\/6) speciálně nakonfigurované pro školy. Cílem bylo ověřit praktickou použitelnost a soulad softwaru s ochranou osobních údajů a v budoucnu nabídnout školám komplexní digitální pracovní platformu. LfDI Dr. Stefan Brink doprovázel pilotní projekt, který trval několik měsíců, poté, co byla společně s ministerstvem přijata rozsáhlá přípravná opatření. Ministerstvu školství a kultury bylo poskytnuto poradenství v otázkách ochrany údajů a zároveň pokračovala jednání se společností Mcrosoft o zlepšení právních a technických rámcových podmínek.

Software vybraný ministerstvem školství má učitelům poskytnout jak e-mailovou službu, tak - jako software jako služba (SaaS) - pracovní prostředí BOro s programy pro zpracování textu, prezentace a výpočty, cloudové úložiště a systém videokonferencí.

Pilotní projekt na školách doprovázel LfDI Dr. Brink, protože přání žáků, rodičů a učitelů po bezpečných a prakticky použitelných digitálních softwarových řešeních bylo v době pandemie obzvláště naléhavé. LfDI chtělo v praxi ověřit, jak skutečně funguje speciální verze MS Office 365, kterou ministerstvo používá, a zda byla provedena i vylepšení, která již byla oznámena v posouzení vlivu na ochranu osobních údajů (DSFA).

Jak však bude vysvětleno, rozsah produktu nakonfigurovaného v pilotním projektu přesáhl rámec fveB, který dříve zkoumalo ministerstvo školství v rámci DSFA. Nicméně mnoho učitelů v pilotních školách si stěžovalo, že funkčnost testovaných služeb byla příliš omezená, zejména že studenti nebyli plnohodnotnými účastníky platformy.

Současné hodnocení testovaného softwaru není průkazné. Řada dalších problematických aspektů nebyla zkoumána; v některých případech se jednalo o

Vzniklé potíže lze také podrobněji prozkoumat. Hloubka zkoumání však již odhalila nedostatky, které vedou k následujícímu doporučení:

V důsledku toho LfDI nedoporučuje používat testované produkty MS ve školním sektoru. Navzdory zvláštním vlastnostem používaných produktů stále existuje velké množství problémů a otevřených otázek, za které nemůže být z hlediska ochrany údajů odpovědné ani ministerstvo školství, ani jednotlivé školy.

Již s ohledem na omezený status testovaný v pilotním projektu, v němž byli informováni pouze učitelé vybraných škol, konstatuje LfDI vysoké riziko porušení práv a svobod dotčených osob. To platí tím spíše pro předpokládané - a v případě digitální vzdělávací platformy pouze samozřejmé - rozšíření systému o účty pro žáky. Na pozadí pozice státu jako garanta, zejména pro pravidelně nezletilé žáky, kteří podléhají povinné školní docházce, LfDI nedoporučuje používat produkty rvticrosoft použité v pilotním testování. Nezdá se být zcela vyloučeno, že další verze výrobků použitých v pilotním testu a za podstatně změněných podmínek použití ve školském sektoru by mohly být použity způsobem, který je v souladu s právními předpisy. Zejména ve školství je však toto používání spojeno s řadou značných rizik, která školy nemohou ovlivnit a která jsou považována za nepřijatelně vysoká vzhledem k obzvláště vysokým ochranným povinnostem.

Poradenská služba LfDI a postup pilotního testu

UDI věnoval mnoho času poradenství a podpoře ministerstva školství a kultury (KM) při vývoji digitální vzdělávací platformy a zejména při využívání systému Mcrosoft (tvS) 365, jak si to KM vyžádalo.

Přehledná časová osa

Ještě před definitivním ukončením projektu ella@bw požádala KM UDI o vyhodnocení využití Microsoft Office 365 jako součásti digitální vzdělávací platformy. První diskuse na toto téma proběhla 8. června 2018 za účasti paní rvtnisterialdirektorin Windey a UDI Dr. Brink.

Dne 3. prosince 2018 se uskutečnilo úvodní setkání UDI a BITBW se zástupci společnosti rvtcrosoft. UDI **poukázal na** potřebu **posouzení vlivu na ochranu osobních údajů (DSFA**). Další jednání mezi KM a UDI
První setkání na pracovní úrovni se uskutečnila na podzim 2019 po vzniku oddělení platformy digitálního vzdělávání Ministerstva školství a kultury.

Po několika jednáních v lednu a únoru 2020 pak KM **koncem dubna 2020** předložil DSFA var, který ÚDI po podrobné analýze začátkem července **zamítl** jako zcela **nedostatečný.**

Na začátku září 2020 KM oznámila, že chce předložit **druhou DSFA** a **držet se projektu**. v důsledku toho a z důvodu časové tísně, na kterou KM pochopitelně upozornila, byly poradenské služby UDI **značně zintenzivněny. Proběhla** řada schůzek, diskusí a videokonferencí, kterých se často účastnili vysoce postavení zástupci společnosti Mcrosoft, včetně členů vedení německé pobočky a zástupců odborných oddělení z USA.

V říjnu 2020 představilo Ministerstvo školství a kultury aktualizovanou a výrazně přepracovanou verzi DSFA var a oznámilo, že ji použije jako základ pro **pilotní provoz,** aby ověřilo praktickou vhodnost M3 365 pro použití ve školách. Revidovaná verze
První DSFA se zabývala pouze omezeným rozsahem produktu.
byly výslovně zahrnuty pouze webové verze, nikoli aplikace pro Android a iOS ani verze pro stolní počítače. DSFA také nevyžadovala, aby studenti měli účet.

Ve stejném období společnost Mcrosoft slíbila rozšířené právní záruky, zejména proti přístupu bezpečnostních orgánů USA. [redacted]

[redacted]

Dne 30. října 2020 oznámil LfDI, že bude pilotní projekt doprovázet jako poradce (https ://Www.baden-wuerttemberg. datenschutz. de/lfdi-begleitet-pilotprojekt-des kultusministeriums- zur-nutzung-von-m icrosoft-office-365-an-schulen/). Stále bylo potřeba DSFA vylepšit, ale LfDI uznal jasně revidovaný dokument jako základ pro pilotní projekt. V praktickém testu se měla otestovat avizovaná vylepšení **MS** 365 a individuální konfigurace ze strany KM.

Dne 17. listopadu 2020 se konala další videokonference, na níž se projednávaly otázky ochrany údajů v souvislosti s realizací pilotního projektu s KM. Následovala další e-mailová korespondence na tato témata.

V lednu 2021 proběhly další konzultace o společném monitorování a hodnocení pilotního projektu s KM a společností Microsoft.

Během probíhajícího pilotního testu provedl LfDI různá technická šetření, zejména pokud jde o datové toky. Dále byl po informování učitelů o dostupnosti LfDI umožněn přístup k fóru, na kterém KM poskytl zúčastněným učitelům možnost diskutovat o problémech a dotazech při práci s pilotovanou službou. Kromě toho KM a LfDI vypracovaly společný dotazník pro hodnocení pilotního projektu.
Zaměstnanci a učitelé zúčastněných škol. Údaje, které **KM** předložil LfDI
LfDI poté vyhodnotil výsledky tohoto průzkumu samostatně.

[redacted]

Ke dni 13. dubna 2021 **KM** zaslala LfDI dokument *"Doplňující připomínka k posouzení vlivu na ochranu osobních údajů týkající se a. implementace Microsoft Office 365 jako SaaS součásti platformy digitální archivace a b. prostředí pro zpracování Office 365.".*
Projekt je srovnáván s projektem "Office 365 ve školách".

Úplný přehled jízdního řádu naleznete v příloze 9 - Marquee.

run.docx

2 Shrnutí základních výsledků

V rámci monitorování pilotního projektu provedl LfDI audit:

- zda byla zmírňující opatření navržená v posouzení vlivu na ochranu údajů (DIA) ministerstva skutečně provedena a zda jsou dostatečná k minimalizaci rizika;
- které se zpracovávají kromě operací požadovaných/požadovaných uživateli (ve vzorcích);
- zda je rozsah funkcí dostatečný a odpovídá očekáváním učitelů;
- zda jsou zakázány i problematické operace zpracování, které jsou považovány za zakázané, např. ty, které jsou zpracovávány v USA, nebo ty, kde MS zpracovává osobní údaje pro své vlastní účely, jako jsou překladové a slovníkové funkce;
- zda by zapečetění mohlo omezit možnost přístupu k datům společnosti Microsoft nebo úspěšných útočníků.

Pilotní projekt byl omezen na prostředí učitele a nezahrnoval školní komunitu nebo umožňoval pouze používání týmů MS bez samostatného účtu pro žáky. Používání MS Teams pro školáky představuje zvláštní výzvu, včetně povinné školní docházky a zvláštní povinnosti státu pečovat o děti vzhledem k jejich věku.

Pro pilotní projekt by měla být použita speciálně nakonfigurovaná verze softwaru, tj. nikoli komerční software, který si může koupit koncový zákazník. Ve speciálně nakonfigurované verzi by měl být přenos telemetrických, diagnostických a dalších dat do členského státu výrazně omezen.

Vícečlenný a intenzivní praktický test ukázal, že tento pokus nebyl úspěšný, že předpoklady se ukázaly jako nepřesné a že používání MS (Office) 365 ve školním kontextu skrývá **řadu nejasných rizik v oblasti ochrany údajů.** Ačkoli nelze vyloučit, že tato rizika bude možné v budoucnu snížit nebo částečně eliminovat - i v rámci konstruktivní síly členských států -, je třeba si uvědomit.
čas také nelze předvídat.

Příklady:

- Pro některá ujednání týkající se provozu školy - zejména převody na společnost Mcrosoft pro **její vlastní obchodní nebo komerční zájmy - neexistuje právní základ.** Školy podléhají tomuto

Právní požadavky v této oblasti jsou mnohem přísnější než u společností používajících produkty MS. Příkladem je kompletní a podrobné sledování a zaznamenávání veškerého chování uživatelů a analýza e-mailů. Sama KM ve svém "Doplňujícím posouzení vlivu na ochranu osobních údajů" ze dne 13. dubna 2021 na straně 10 správně označuje existenci odpovídajícího právního základu za spornou.

- **Deaktivaci** problematického **zpracování** osobních údajů nebo **zpracování, které je výslovně vyloučeno z** působnosti zákona o ochraně osobních údajů KM, bylo možné **zjistit pouze částečně**.

- V případě zpracování **zvláštních kategorií údajů** podle článku 9 GDPR, jako jsou údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, údaje o zdravotním stavu nebo údaje týkající se sexuálního života nebo sexuální orientace fyzické osoby, nezletilých osob, které podléhají zvláštní ochraně, je **obtížné si představit, jak lze zvládnout vysoká rizika pro práva a svobody subjektů údajů.**

- Existuje řada **přenosů dat do USA,** kterým nelze zabránit. Z toho vyplývají i velká rizika ve světle rozsudku Evropského soudního dvora ze dne 16. července 2020 ve věci C-311/18 ("Schrems II"). Uvidíme, jaká další rozhodnutí ohledně přípustnosti předávání údajů do USA přijme Konference o ochraně údajů (DCC) jako sdružení dozorových orgánů jednotlivých států a federální vlády, Evropský výbor pro ochranu údajů (EDSA) a nakonec Evropský soudní dvůr (ESD). Rizika spojená s takovými přenosy by mohla být zmírněna odůvodněnými dodatečnými zárukami, které společnost Microsoft poskytla ke standardním smluvním ustanovením dodatku o ochraně údajů ke službám Mero soft Online (dále jen "D PA"), avšak nikoliv definitivně odstraněna. To je o to znepokojivější, že převody do třetích zemí mají i v pilotní variantě softwaru stále velký rozsah.

- Podle plánu KM se má okruh uživatelů výukového softwaru **rozšířit** i na **žáky,** jak si přáli dotazovaní učitelé. Tato touha po rozšíření j e v kontextu efektivního využívání vzdělávací platformy zcela zřejmá. Z hlediska ochrany údajů je však riziko v současné konstelaci značně zvýšené. KM rovněž předpokládá, že tomu tak je,

že zpracování výše uvedených zvláštních kategorií osobních údajů ve vzdělávací platformě není při používání zde používané služby MS přípustné a zakazuje jej prostřednictvím **pravidel používání.** Z průzkumu mezi učiteli (Příloha 6 - Vyhodnocení průzkumu k pilotnímu projektu MS Office MŠMT) však vyplývá, že toto opatření zákazu pomocí pravidel používání není dostatečně účinné. **Pokud je toto opatření již**

Pokud nestačí učitelům, lze předpokládat, že je zcela nevhodná pro žáky.

- Zvláště problematické **telemetrické a diagnostické údaje** nebylo možné v průběhu pilotního projektu deaktivovat nebo omezit. Podle našich zjištění dochází k předávání diagnostických, telemetrických nebo jiných osobních údajů uživatelů společnosti Microsoft (v tomto případě je příslušná škola považována za správce ve smyslu čl.4 odst.7 GDPR) a k dalšímu zpracování těchto údajů společností Microsoft pro vlastní účely formou **pozorování, zaznamenávání a vyhodnocování chování uživatelů a zařízení bez rozpoznatelného právního základu, a to** i nadále v rámci provozu šarže a ve velmi velkém rozsahu, který není nezbytný pro poskytování služby. Zejména možnosti nastavení v rámci MS 365 pro deaktivaci jsou v podstatě omezeny na desktopové verze (které nejsou zahrnuty do oblasti působnosti DSFA) a nezahrnují **online/webové verze MS 365** (určené pro použití KM).

- I přes rozsáhlé úsilí LfDI při přímých jednáních se zástupci společnosti Microsoft **se nepodařilo získat** úplný **přehled o veškerém zpracování osobních údajů** (včetně zpracování pro vlastní účely společnosti Microsoft).

- V průběhu pilotního projektu bylo zjištěno, že **nápravná opatření, která byla v** KM DSFA označena za **zásadní, nebyla plně provedena a v některých případech nebyla provedena vůbec,** jako například nápravná opatření "end-to-end" a "privacy by default".

- **Nebylo nalezeno žádné šifrování, které by** technicky vyloučilo nebo výrazně omezilo přístup společnosti Mcrosoft, jejích zaměstnanců nebo jejich subdodavatelů či úspěšných útočníků k osobním údajům. Během pilotního provozu se nepodařilo zjistit, že by uživatelé měli **kontrolu nad správou klíčů** jakéhokoli stávajícího šifrování.

- [redacted]

3Technické testování

Na podzim roku 2020 poskytly KM, BrTBW a zúčastnění poskytovatelé dílčích služeb LfDI pět testovacích účtů. Tyto účty odpovídaly běžným účtům učitelů. Ke konci testovací fáze byla jednomu testovacímu účtu přidělena role "Global Reader", aby mohl zobrazovat nastavení (ale ne data).

Tyto účty byly použity k různým funkčním testům a k analýze příslušného datového provozu.

Za účelem testování online aplikací pro telemetrická a diagnostická data, jakož i otázky, zda MS zpracovává další, případně jinak určená uživatelská data, byl veškerý datový provoz zaznamenán a analyzován pomocí mitmproxy nebo BurpSuite. Vzhledem k tomu, že KM v průběhu procesu rozhodla, že v pilotním provozu bude využívána pouze online verze MS 365 v prohlížeči, nebylo pokračováno v započatém testování aplikací pro Android a iOS.

Kromě protokolování pomocí mproxy/BurpSuite byly odebrány vzorky pomocí vývojářských nástrojů Firefoxu, které potvrdily všechny naměřené datové toky.

V průběhu auditu byly v několika relacích prováděny různé činnosti, od počáteční registrace až po zpracování dokumentů.

Podrobnosti o auditu, včetně seznamů kontaktovaných hostitelů a zjištěných telemetrických údajů, jsou uvedeny v *příloze* 7 - *Technická analýza.*

Pohled shora technický Nedostatek

Bylo zjištěno několik technických problémů (viz *Příloha 1 - Zjištění MS365--Technické), které byly vzneseny vůči* společnosti Microsoft na schůzce dne 6. dubna 2021, aniž by byly problémy k uvedenému datu vyřešeny. Jedná se o tyto otázky:

- Rozsáhlé **datové toky** z MS 365, z nichž většina **není zdokumentována** v dokumentech DSFA MŠMT. Často není srozumitelné, k jakým účelům rozsáhlé zpracování osobních údajů slouží, které kategorie údajů zahrnují a proč je toto zpracování nezbytné pro účely příslušné školy. Během celého zkušebního období byla identifikována připojení k přibližně 500 různým serverům (hostitelům) společnosti Microsoft, z nichž je zdokumentováno pouze asi 50 (podrobnosti viz *Příloha* 7 - *Technická analýza).*

- Při používání MS 365 **jsou osobní údaje popsané** různými pojmy, které však **nejsou podrobně uvedeny, poskytovány** společnosti MS a zpracovávány **pro** (jak MS říká) "**oprávněné podnikání společnosti Microsoft" nebo "oprávněné podnikání společnosti Microsoft".**

  ted. Mimo jiné jsou označovány jako telemetrické nebo diagnostické údaje nebo jsou popisovány jinými termíny (např. jako "údaje generované službou" nebo "základní služby"), aniž by byl srozumitelně vysvětlen přesný rozsah zpracovávaných údajů. Některé z těchto údajů jsou van Mero
  soft dokumentace, kompletní dokumentace všech zpracovaných per
  Neznáme podrobnosti o údajích, datových tocích a rozsahu zpracování (např. události), jejich účelu a nezbytnosti, odpovědnosti a právním základu. Ministerstvo kultury a Mero soft byly již v říjnu 2020 požádány o popis 26 vzorových datových toků (viz *Příloha 10 - Popis vzorových datových toků* a *Příloha 11 - Vzor dokumentace datových toků a událostí)*, popis zatím není k dispozici (k 23. 4. 2021).

  -Zpracování údajů je proto v tomto ohledu netransparentní. [redacted]
  právní základ pro údaje
  Takto rozsáhlý přenos osobních údajů ve školním prostředí není pro LfDI proveditelný.

- Vzhledem k tomu, že LfDI během příprav pilotního **provozu** zjistil, že aplikace Mcrosoft Authenticator obsahuje **přenosy dat poskytovatelům reklamních služeb, mělo** být její používání během pilotního provozu deaktivováno. Přesto byli uživatelé vyzváni, aby místo alternativy "FreeOTP" zkoumané v DSFA používali aplikaci Mcrosoft Authenticator.

- Při používání služby Microsoft 365 v rámci digitální vzdělávací platformy museli uživatelé v některých bodech **souhlasit se "Zásadami ochrany osobních údajů" společnosti Microsoft**. **Při používání služby Microsoft 365 jako součásti digitální vzdělávací platformy** byli **uživatelé na některých místech** povinni souhlasit **s "Prohlášením o ochraně osobních údajů" společnosti Microsoft** a/nebo **se všeobecnými podmínkami**, **"Podmínkami používání" nebo "Smlouvou o poskytování služeb společnosti Microsoft"**, případně na ně byli odkázáni s tím, že se na ně vztahují. To vyvolává otázku, zda mohou uživatelé státní platformy souhlasit se zpracováním údajů soukromou společností a zda je tento souhlas dobrovolný (viz EC 43 GDPR). Kromě toho se tímto způsobem snažíme objasnit právní vztahy, které jsou samy o sobě relevantní (uživatelský vztah mezi uživatelem a školou, který je zase právním vztahem mezi uživatelem a školou).

(např. pokud uživatel uzavřel s KM smlouvu o zpracování, přičemž KM využívá MS jako dílčího zpracovatele) na základě přímého smluvního vztahu nebo souhlasu mezi uživatelem a MS. To vede k další netransparentnosti, což je podle názoru LfDI nepřijatelné.

- Přestože podle DSFA by mělo být používání všech aplikací kromě verzí prohlížeče deaktivováno, bylo možné během pilotního provozu používat verze aplikací Outlook, Word, Excel atd. pro systémy iOS a Android. To je obzvláště důležité u aplikace Outlook, protože umožňuje používat libovolnou e-mailovou adresu.
  Služby společnosti Microsoft mimo Microsoft 365 (např. soukromý e-mailový účet učitele) lze používat, ale v tomto případě jsou **všechny e-maily tohoto účtu zpracovávány na serverech společnosti Microsoft** a **hesla uživatelů** jsou **zpracovávána společností Microsoft v čistém textu.** Tento
  To může být v mnoha situacích porušením bezpečnostních požadavků na IT, a to i mimo problém ochrany údajů, který spočívá v nadřazeném zpracování osobních údajů.

- Vzhledem k tomu, že **pouze online/webové verze** aplikací van Mcrosoft 365 a MS Teams byl zobrazen ve webovém prohlížeči, mělo být používání desktopových verzí těchto aplikací zakázáno. Přesto bylo možné v pilotním projektu použít desktopovou verzi MS Tean1s. Zpracování a rizika s tím spojená však nebyla zohledněna.

- Ačkoli by měly být **převody do třetích zemí z** velké části vyloučeny, testy provedené LfDI v rámci vzdělávací platformy odhalily velmi vysoký počet převodů do třetích zemí - především do USA. Neexistuje pro to žádný právní základ, zejména pro veřejné orgány.

- Nebylo možné objasnit, zda společnost Mcrosoft umožňuje školám dostatečně chránit **práva subjektů údajů** podle článku 15 GDPR.

- Není jasné, zda je možné zaručit **důvěrnost komunikace v** potřebném rozsahu. To se týká jednak otázky, které komunikační údaje společnost Mcrosoft zpracovává pro své vlastní účely (např. boj proti spamu a milwaru), a jednak toho, zda je lze dostatečně chránit před přístupem cizích tajných služeb. Poskytovatel nedodržuje technickou směrnici Spolkového úřadu pro bezpečnost informací "Bezpečný přenos e-mailů" (BSI TR-03108).

4Vyhodnocení právních rizik

Studie a hodnocení reálných rizik zmíněné na začátku byly provedeny se zvláštním zaměřením na situaci škol a orgánů veřejné správy.

o tom, do jaké míry je Microsoft 365 v konfiguraci Ministerstva školství a kultury v souladu se zásadami pro zpracování osobních údajů z článku 5 Nařízení, lze pochybovat, a to zejména v oblasti školství s ohledem na právo na výchovu a vzdělávání a zvláštní právo na ochranu nezletilých.

- osobní údaje jsou zpracovávány zákonně, korektně a způsobem srozumitelným pro subjekt údajů (čl. 5 odst. 1 písm. a) Nařízení),
- osobní údaje jsou shromažďovány pro konkrétní, výslovně vyjádřené a legitimní účely a nikoli způsobem, který je s těmito účely neslučitelný.
  - (čl. 5 odst. 1 písm. b) nařízení),
- operace zpracování jsou přiměřené a omezené na to, co je nezbytné pro účely zpracování (čl. 5 odst. 1 písm. c) GDPR); a
- osobní údaje jsou uchovávány ve formě, která umožňuje identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou údaje zpracovávány (čl. 5 odst. 1 písm. e) nařízení).

Aspekty školského práva a zvláště chráněné Oaten

Je třeba poznamenat, že zejména školy musí splňovat zvláště vysoké požadavky na ochranu údajů, které vzhledem k uvedeným problémům nelze považovat za splněné. hZpracování osobních údajů, ke kterému ve školách nevyhnutelně dochází, je zvláště hodné ochrany z následujících důvodů:

- Většina žáků vzdělávaných ve školách jsou nezletilé osoby, které jsou pod zvláštní ochranou státu a jejichž zvláštní potřebu ochrany při zpracování jejich osobních údajů uznává i základní nařízení o ochraně osobních údajů (viz.
  např. 38., 58., 65., 71. a 75. bod odůvodnění, čl. 6 odst. 1 písm. f).
  poslední polovina věty, článek 8, čl. 12 odst. 1, druhá polovina věty, čl. 57 odst. 1 písm. b) ODR a následně § 14 odst. 1 bod 2 BOSG).

- Učení ve škole zahrnuje svobodu, kreativitu, zkoušení hranic a možnost dělat chyby. Tato svoboda, která je pro vzdělávání nezbytná, nesmí být ohrožena nejasnou ochranou zpracovávaných údajů.

- Veřejné školy plní suverénní úkoly. Zpracování osobních údajů dotčených osob v rámci plnění veřejného úkolu (např. formou předání třetím stranám, jako je v tomto případě členský stát) proto nemůže být založeno na žádném oprávněném zájmu správce údajů (čl. 6 odst. 1 druhý pododstavec GDPR). Takto to zřejmě vidí i MŠMT, neboť právní základ pro předávání osobních údajů z působnosti MŠMT nebo jednotlivých škol zůstává sporný i pro MŠMT (viz str. 10, "Doplňující úvaha k posouzení vlivu na ochranu osobních údajů", MŠMT ze dne 13. 4. 2021). Bez tohoto právního základu však není vyšetřování přípustné.

- Na žáky se vztahuje převážně povinná školní docházka, za kterou v případě nezletilých odpovídají také rodiče nebo zákonní zástupci. Vzhledem k tomuto jasnému vztahu nadřízenosti a podřízenosti není zpracování údajů na základě souhlasu obvykle možné (42. a 43. bod odůvodnění GDPR).

- Školáci mají zároveň právo na vzdělání zaručené v článku 13 Mezinárodního paktu o hospodářských, sociálních a kulturních právech (dále jen "Sociální pakt OSN"), v **článku** 28 Úmluvy OSN o právech dítěte, v článku 11 Ústavy spolkové země Bádensko-Württembersko a ve školském zákoně spolkové země Bádensko-Württembersko (zejména v § 1), které nesmí být narušeno nedostatečnou ochranou údajů. Naplnění tohoto práva (na vzdělání) nesmí být závislé na souhlasu. Ministerstvo školství a kultury by však v této oblasti chtělo pracovat zejména se souhlasem (viz str. 10, "Doplňující úvaha k posouzení vlivu na ochranu osobních údajů", Ministerstvo školství a kultury, 13. dubna 2021).

- Ve školách se zpracovává velké množství zvláště citlivých údajů, které získávají rozsáhlé poznatky zejména o osobě a osobních poměrech žáků a v některých případech i jejich rodin. Patří mezi ně zejména "zvláštní kategorie osobních údajů", které obecné nařízení o ochraně osobních údajů považuje za údaje vyžadující zvláštní ochranu, jako jsou údaje o etnickém původu, politických názorech, náboženském vyznání atd., jakož i údaje týkající se jednotlivce.

nebo filozofické přesvědčení, jakož i údaje o zdravotním stavu nebo údaje týkající se sexuálního života či sexuální orientace (článek 9 GDPR). Školy však ve velkém rozsahu zpracovávají i údaje, které jsou jinak považovány za zvláště citlivé a u nichž lze v případě porušení ochrany pravidelně předpokládat vysoké riziko pro individuální práva a svobody fyzických osob, jako jsou údaje o sociální situaci obecně a (například v souvislosti se školními známkami a jiným hodnocením) údaje o hodnocení nebo klasifikaci jednotlivců a jejich výkonů (srov. např. 75. bod odůvodnění základního nařízení o ochraně osobních údajů). V ojedinělých případech zpracovávají školy také údaje podléhající zvláštní ochraně (rozšířené) ochrany sociálních údajů podle § 78 SGB X.

V této souvislosti stojí za zmínku, že samotná DSFA KM ze dne 16. října 2020 ji popisuje jako Je "zřejmé", že při používání MS 365 jako softwaru jako služby (SaaS) v rámci vzdělávací platformy bude sdělování zvláštních kategorií údajů podle čl. 9 odst. 1 GDPR zakázáno předpisy o používání nebo příslušnými správními předpisy (viz str. 16 v poznámce pod čarou č. 14). 16 v poznámce pod čarou č. 14), a také to doporučil jako nezbytnou záruku pro využívání této služby v rámci vzdělávací platformy (viz např. str. 57 na konci návrhu smlouvy mezi příslušnou školou a KM a v samotném textu návrhu nařízení o používání na str. 99, "5. Normativní požadavky na zpracování osobních údajů").

Z toho vyplývá, že ani podle KM neposkytuje služba dostatečné záruky pro zpracování zvláštních kategorií osobních údajů a že jejich zpracování je třeba zabránit organizačními opatřeními v podobě zákazu zpracování. Nicméně i obecný zákaz zpracování typů údajů uvedených v článku 9 GDPR ve vzdělávací platformě se zdá být neproveditelný, protože školy jsou na možnosti zpracovávat i tyto typy údajů závislé. Kromě toho pouhé uvedení zákazu používání v předpisech neposkytuje dostatečnou jistotu, že tento zákaz bude dodržován. Průzkum mezi učiteli, kteří se zúčastnili pilotního provozu, například ukázal, že přibližně 1/6 učitelů nenašla předpisy. Například průzkum mezi učiteli, kteří se zúčastnili pilotního projektu, ukázal, že přibližně 1/6 učitelů předpisy nenašla nebo nečetla. Tato skupina učitelů spolu s těmi, kteří pravidlům nerozuměli nebo jim alespoň nerozuměli, tvořila dobrou třetinu učitelů, kteří se průzkumu zúčastnili.

Navíc, i kdyby byl dodržen, úplný zákaz zpracování zvláštních kategorií osobních údajů ve smyslu článku 9 obecného nařízení o ochraně osobních údajů by nebyl dostatečným řešením nedostatků služby z hlediska ochrany údajů. Je tomu tak proto, že mezi údaji zpracovávanými školami - jak bylo vysvětleno výše v posledním bodě - vyžadují zvláštní ochranu nejen zvláštní kategorie osobních údajů, ale také celá řada dalších typů údajů, které jsou zpracovávány ve velkém rozsahu, jako jsou sociální údaje nebo údaje o hodnocení či klasifikaci osob a jejich výkonnosti. V tomto ohledu KM DSFA rovněž uznala, že zde existuje velká potřeba ochrany, a proto doporučila vyslovit další zákazy v uživatelských předpisech. Konkrétně by podle doporučení OSFA měly být ze zpracování vyloučeny mj. tyto osoby

- "údaje, které umožňují vyvozovat závěry o osobních charakteristikách, jež úzce souvisejí se zárukou lidské důstojnosti"; a

údaje, které ve spojení s dalšími údaji umožňují vytvoření osobnostního profilu (zejména údaje o výkonu)", ten však "pouze v případě, že konkrétní komunikační proces obdrží několik takových údajů" (s. 87 DSFA ze dne 16. října 2021).

Toto doporučení však nebylo provedeno v pravidlech používání, která byla skutečně navržena a používána: Ačkoli pravidla obsahovala zákaz zpracování zvláštních kategorií osobních údajů, neobsahovala výše uvedené zákazy zpracování. V každém případě se zdá, že je pro učitele velmi náročné, pokud se od nich očekává, že budou při používání platformy zohledňovat tyto interpretační skutečnosti, aby mohli rozhodnout o přípustnosti použití.

Rovněž se zdá být sporné (na pozadí výše uvedeného příplatku za zvlášť citlivé údaje, které se ve školách skutečně zpracovávají), zda další dva body uvedené v DSFA skutečně vylučují všechny údaje vyžadující vysokou úroveň ochrany. Kromě již v úvodu zmíněných typů údajů (jako jsou údaje o hodnocení nebo klasifikaci osob a jejich výkonnosti) je třeba mít na paměti, že obecné nařízení o ochraně osobních údajů, jak bylo vysvětleno výše, již vnímá zvláštní potřebu ochrany při zpracování osobních údajů dětí, což KM DSFA na začátku uznala (str. 16 a 78), ale při zkoumání dostatečnosti nápravných opatření se jimi dostatečně nezabývala.

A konečně, zákaz zpracování zvláště citlivých osobních údajů by byl pro jejich ochranu zcela nedostatečný, pokud by - což musí být nakonec cílem a bylo to také zjevně žádoucí ze strany vedení škol a učitelů, s nimiž byly vedeny rozhovory v rámci pilotního projektu - měli žáci sami získat účet pro účast ve vzdělávací platformě. Zákaz namířený proti těmto žákům by nebyl cílený ani dostatečný k tomu, aby jim zabránil zveřejňovat takové osobní údaje o sobě nebo o jiných ve svých prohlášeních o platformě. Pokud by navíc taková prohlášení byla učiněna v soukromých chatech nebo jiných formách komunikace pouze mezi žáky, mohla by škola dodržování takového zákazu jen stěží vynutit.

Souhrnně lze říci, že DSFA je k dispozici pouze u rizik s počty akcelerátorů pro učitele a u služby se značně omezenou funkčností (např. bez aplikací a desktopových aplikací), jejíž navrhovaná 1\/aBopatření ke zmírnění rizik jsou také částečně pochybně účinná. Zde jsou důležité otázky, a tedy i rizika, stále nejasné. Ze strany učitelů existuje silná poptávka po zapojení studentů. Digitální vzdělávací platforma bez žáků se nezdá být příliš efektivní.

Průzkum KM, do něhož mohl LfDI přispět otázkami, ukazuje, že všechny zúčastněné školy jsou již vybaveny E-1\/ail. Velmi častý je mezi nimi také systém pro řízení výuky (tv1oodle) a videokonferenční systém (BigBlueButtan) (14 z 23 škol, tj. 60 %). Tyto služby často využívá BelWO (e-mail, M>odle v 60 %) a Zentrum tor Schulqualitat und Lehrer bildung Baden-WOrttemberg (ZSL, BigBlueButton - v 11 z 23, tj. cca 50 % - s přímým propojením na tv1oadle v BelWO). Pokud je nám známo, KM již investovala finanční prostředky do rozšíření kapacit BelWO a ZSL. Podle našich zjištění již nějakou dobu probíhá také školení učitelů v používání aplikací provozovaných v BelWO a ZSL. V této souvislosti se změna rizikové služby 1\/18 pro školský sektor nejeví jako nezbytně nutná.

K rozsudku ESD ve věci "Schrems 11"

Mezinárodní předávání údajů z Evropy do USA je po rozhodnutí Evropského soudního dvora ve věci Schrems II v červenci 2020 možné jen ve velmi omezené míře, ačkoli řada amerických poskytovatelů je ústředními hráči v globálním zpracování údajů.

Jedním z důvodů je názor Evropského soudního dvora, že masové sledování ze strany amerických bezpečnostních agentur, jako je NSA, je zcela nadměrné, a proto mohou být údaje Evropanů nyní předávány do USA pouze na základě dodatečných ochranných opatření.

V listopadu 2020 předložil Mcrosoft jako jeden z *ústředních* poskytovatelů globálně propojených IT produktů řadu návrhů záruk, které přímo posilují práva uživatelů a které byly zásadně odůvodněny LfDI (#DSGVOwirkt:
Společnost Mcrosoft se přizpůsobuje evropské ochraně údajů | Státní komisař pro ochranu údajů
ochrana a svoboda informací Bádensko-Württembersko).

Nové smluvní doložky společnosti Mcrosoft obsahují ustanovení o

- právo na odškodnění subjektu údajů, jehož údaje byly zpracovány protiprávně a který v důsledku toho utrpěl majetkovou nebo nemajetkovou újmu;

- informování subjektu údajů, pokud je společnost Mcrosoft na základě vládního příkazu ze zákona povinna poskytnout informace bezpečnostním orgánům USA; a

- povinnost společnosti Mcrosoft podat žalobu u soudů v USA a napadnout správní příkaz k předání údajů.

Problém předávání údajů do USA to obecně neřeší - dodatek ke standardním smluvním doložkám totiž nemůže vést k zamezení přístupu amerických tajných služeb k údajům, což Evropský soudní dvůr kritizoval jako nepřiměřené. Je to však nepochybně krok správným směrem.

[redacted]

Samit posunul společnost Mcrosoft směrem k dodržování ochrany osobních údajů a spolupracoval s ní.

Používání softwaru způsobuje problémy, které uživatelé s méně složitými nabídkami z EU nemají. To ponechává značné nejistoty, zejména při využívání amerických poskytovatelů služeb: Vzhledem k rozhodnutí Evropského soudního dvora ve věci Schrems 11 z července 2020 je v současné době často nejasné, jak bude v budoucnu legální předávání údajů z EU do USA. A tato otázka se nebude řešit v Bádensku-Wortenbersku, ale nakonec na evropské úrovni.

Obecně platí, že *u* velké části zpracování údajů společností Mcrosoft existují nejasnosti týkající se oddílu 702 *zákona o* dohledu nad zahraničním zpravodajstvím (FISA), směrnice prezidenta č. 28 (PPD-28), *zákona* USA PATROT *Act a* výkonného nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.
12333 nebo -US CLOUD *kt.* Takové nejasnosti je třeba odstranit, pokud z
Orgány veřejné moci chtějí s citlivými údaji nakládat zodpovědně, například ve školství.

Zohlednění zejména kritických bodů OSK

LfDI úzce spolupracuje s Konferencí státních a federálních dozorových orgánů (OSK), která plní úkoly v oblasti ochrany údajů, na objasnění posouzení ochrany údajů u služeb.

Uzavření smlouvy - Situace

Za současného stavu existují značná rizika, která podle názoru LfDI nemůže nést správce ve školském sektoru. zejména tyto jednotlivé školy mají jako správci pouze nedostatečný vliv na podobu používaných produktů a u dohod uzavřených za tímto účelem existuje rozpoznatelné riziko, že nebudou právně odrážet skutečné okolnosti zpracování. Ten je

Nicméně - také podle nových pokynů Evropského sboru pro ochranu osobních údajů (k dispozici na adrese: https://edpb.europa.eu/s ites/edpb'files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, s. 11 a násl.) - nezbytné pro účinná smluvní ujednání v kontextu **článku** 26 nebo 28 GDPR.

5 Závěrečné poznámky

Celkově vzato **si ani LfDI, ani správce** údajů **nemohou být jisti,** že velmi rozsáhlý sběr uživatelských údajů zdokumentovaný v pilotním projektu probíhá **legálně a že lze účinně vyloučit nezákonné zpracování.** Naopak existuje řada spolehlivých indicií, že osobní údaje uživatelů jsou zpracovávány, v některých případech ve velkém rozsahu, bez rozpoznatelného právního základu.

Školáci, rodiče a učitelé chtějí právně bezpečnou a funkční vzdělávací platformu. Záměr KM využít pro vzdělávací platformu velmi výkonného poskytovatele je proto pochopitelný, a to i na základě získaných zkušeností. Intenzivní praktická zkouška, která trvala několik měsíců, však ukázala, že

Odpovědné osoby (čl. 4 č. 7 GDPR) **nemají úplnou znalost zvoleného systému.**

Kontrola nad celým systémem a procesorem.

Do společnosti Mcrosoft proudí mnoho nekontrolovatelných dat. Ačkoli společnost Mcrosoft konstruktivně podpořila celkový proces KM, **nebyla schopna poskytnout dostatečné informace a jasnost,** když byla dotázána na kritické body nebo datové toky. Podle GDPR je však znalost daného zpracování nezbytným předpokladem pro to, aby správce mohl plnit své povinnosti podle čl. 5 odst. 2 GDPR: Odpovídá za dodržování zásad zpracování osobních údajů a musí být schopen to také prokázat (odpovědnost).

I přes rozsáhlé úsilí LfDI, včetně přímých rozhovorů s vysoce postavenými představiteli společnosti Microsoft, se nepodařilo získat úplný přehled o veškerém zpracování osobních údajů (včetně zpracování pro vlastní účely společnosti Mcrosoft). Jestliže se ani MŠMT s intenzivní podporou ÚDI nepodařilo přes velké úsilí, vysoký personální vklad a přístup ke zkušeným technikům Microsoftu během pilotního provozu dosáhnout dostatečného vyjasnění datových toků, právních základů a technických opatření poskytovatele, lze **si jen těžko představit, že to jednotlivé školy zvládnou lépe.** Jelikož však za zpracování školních údajů odpovídají školy, je těžké si představit, jak by mohly postupovat lépe.

Pokud jsou subjekty údajů správci údajů a v tomto ohledu zaujímají pozici ručitele, vzniká nevyřešený problém s ochranou údajů ve smyslu čl. 5 odst. 2 nařízení GDPR.

Zvláštní pozornost je třeba věnovat výše uvedeným bodům, pokud jde **o údaje o** školácích, tj. nezletilých. Zpracovávají se osobní údaje dospívajících, kteří se musí nejprve naučit najít a vyjádřit svůj názor v chráněném prostředí školy. To nevyhnutelně zahrnuje také

problematické situace, které by neměly opustit omezený prostor školy nebo třídy a musí být řešeny pedagogicky. Zde je třeba zdůraznit povinnost státu chránit.

Podle názoru LfDI se tato rizika při používání výrobků použitých v pilotním projektu jeví jako nepřijatelně vysoká.

Proto se doporučuje **minimalizovat rizika.** Jednou z forem minimalizace rizik může být **využití technických řešení, která mohou být omezená, jako jsou** ta, která již KM používá a která byla vyvinuta v posledních několika letech s využitím finančních zdrojů.
byly úspěšně vyvinuty a podle nejlepšího vědomí UDI byly zachovány. Mezi technická řešení používaná ve školách patří systém pro řízení výuky rvbodle v BelWO a videokonferenční systém BigBlueBut ton v Centru pro kvalitu škol a vzdělávání učitelů (2SL). BigBlueButton se dobře integruje s aplikací Moodie. Předchozí poptávka po alternativních řešeních by mohla být také
Systém je doplněn dalšími službami, jako je cloudové úložiště a online zpracování dokumentů. Například Nextcloud od stejnojmenné stuttgartské společnosti a Onlyoffice nabízí odpovídající open source software. Další softwarová řešení a podporu nabízejí společnosti v Bádensku-Wortenbersku, Německu i mimo něj. Udržitelné rozšíření těchto a dalších technicky kontrolovatelných alternativ může vést k velmi efektivní a odolné digitální vzdělávací platformě.

Závěrem bychom rádi **upozornili, že** UDI nebude během letních prázdnin provádět žádné kontroly ve školách z vlastní iniciativy s cílem zakázat výrobky; od začátku nového školního roku však bude důsledně prošetřovat všechny stížnosti, které v té době obdrží.

6 Přílohy

Název souboru	Popis
Příloha 1 - Nález s-MS365--Technical.pdf	Přehled technických nedostatků: Průběžné technicko-organizační testování Microsoft Office 365 v rámci pilotního projektu MŠMT na využití Microsoft Office 365 ve školách. Tento dokument byl zaslán společnosti Microsoft a projednán s ní na slyšení dne 6.4.
Příloha 2- Analýza M Authenticator Andro id.pdf	Analýza komunikace aplikace MS Authenticator v systému Android.
Příloha 3- Analýza aplikace Outlook Android a iOS prostřednictvím IMAP a SMTP.pdf	Analýza komunikace aplikace Outlook pod systémy Android a iOS s poštovními servery kromě Microsoft 365.
Příloha 4- Krátký test Word Android.pdf	Krátký test Word pod Androidem.
Analýza 5- Krátký test Office Android.pdf	Krátký test Office v systému Android.
Příloha 6- Vyhodnocení průzkumu k pilotnímu projektu MS Office MŠMT.pdf	Vyhodnocení LfDI původní otázky Ministerstva kultury mezi školami zapojenými do pilotního projektu
Příloha 7-Technická analýza.pdf	Informace a výsledky technické analýzy, včetně seznamu všech křestních jmen, která služba kontaktovala v rámci testů LfDI, a přehledu předaných událostí.

Název souboru	Popis
Příloha 8 - Opravné prostředky.pdf	Tabulka s nápravnými opatřeními uvedenými v posouzení vlivu na ochranu osobních údajů KM a způsob, jakým byla provedena.
Příloha 9 - Časový harmonogram.pdf	Hrubý přehled chronologického sledu poradenských služeb LfDI
Příloha 10- Vzorový popis datového souboru.pdf	Popis 26 příkladných datfl0s sen, jejichž obsah a význam není objasněn.
Příloha 11 - Šablona dokumentace toků dat a událostí.docx	Vzory pro popis datových toků, zejména telemetrických a diagnostických dat.