**Doporučené standardy a úroveň zabezpečení na *Lepařovo gymnázium, Jičín, Jiráskova 30*** **v oblasti IT v souvislosti s nařízením GDPR**

## 1/ Přístup k osobním údajům

|  |  |
| --- | --- |
| **Doporučené zabezpečení osobních údajů podle jejich způsobu uložení** | |
| Osobní údaje jsou uloženy přímo na pevném disku daného počítače | * počítač musí být přístupný pouze na heslo/uživatelské jméno, které je individuální pouze pro osobu oprávněnou k přístupu k osobním údajům (tj. nikoliv např. sdílené heslo pro všechny učitele) * počítač musí být v době, kdy je nepoužívaný/vypnutý, v uzamčené místnosti |
| Osobní údaje jsou uloženy na serveru (ve sdílené složce) - tedy potenciálně dostupné z jakéhokoliv počítače ve školní síti | * musí být zajištěno, že osobní údaje jsou dostupné pouze oprávněným osobám (tj. do sítě je potřeba se hlásit na konkrétní uživatelský účet/jméno nebo složka musí být dostupná pod heslem, které je známé pouze příslušné oprávněné osobě) * server by měl být ve speciální zamčené místnosti s přístupem pouze pro nezbytný okruh osob (ředitel, IT technik) * data na serveru by měla být šifrovaná |
| Osobní údaje jsou uloženy v cloudu (potenciálně dostupné z jakéhokoliv počítače či mobilního zařízení) | * všechny počítače či mobilní zařízení, která jsou využívána pro přístup k osobním údajům, musí být řádně zabezpečena - musí vyžadovat heslo pro přístup * přístup k souborům by měl být chráněn heslem, které je potřeba zadat při každém novém přihlášení do cloudové služby (tj. nikoliv “zapamatovat heslo”) * je potřeba mít s poskytovatelem cloudové služby uzavřenou dohodu/smlouvu dle požadavků GDPR |
| Osobní údaje jsou uloženy ve speciálním software (např. Bakaláři, Škola online, účetní systémy apod.) | * všechny počítače či mobilní zařízení, která jsou využívána pro přístup k osobním údajům, musí být řádně zabezpečena - musí vyžadovat heslo pro přístup * systém by měl umožňovat individualizovaný přístup pro jednotlivé uživatele, a nastavení práv tak, aby bylo možné nastavit každému práva pouze na určitou oblast (tj. nikoliv jedno společné heslo a přístup pro všechny) * je potřeba mít s poskytovatelem systému uzavřenou dohodu/smlouvu dle požadavků GDPR |

**Obecná doporučení ke všem typům uložení osobních údajů**

* osobní údaje je potřeba ukládat pouze do složek a programů k tomu určených - nelze např. přenášet na flash-disku v nezabezpečené podobě
* při zasílání emailem doporučujeme soubor zaheslovat a heslo sdělit příjemci jinou cestou (např. formou sms)
* při každém opuštění počítače, na kterém probíhá práce s osobními údaji, musí dojít k jeho“uzamknutí” tak, aby při návratu k počítači bylo nutné opět zadat heslo
* ať už se jedná o přístup do počítačové sítě nebo do speciálního software, zajistí individualizované osobní účty transparentnost v nakládání s osobními údaji - v případě úniku dat se dá vysledovat k jakému konkrétnímu pochybení došlo (pokud přistupují všichni pod jedním účtem/heslem - je jakékoliv vysledování příčiny problému téměř nemožné)
* používat svěřené zařízení výpočetní techniky pouze pro pracovní účely (tj. nestahovat soubory pro soukromé účely (např. filmy, dokumenty apod.) na disk počítače

## 2/ Doporučení k tvorbě hesel

* heslo musí obsahovat minimálně 8 znaků
* mělo by se jednat o kombinaci velkých a malých písmen a čísel nebo speciálních znaků
* neměla by obsahovat “slovníková” slova - např. “Skola123”
* měla by být nastavena pravidelná změna hesel, minimálně 2 x za rok
* hesla by se neměla psát nikam na papír a ukládat poblíž počítače
* heslo pro přístup do počítače by mělo být jiné než heslo pro přístup do softwaru/aplikace s osobními daty (tak, aby se pro přístup k osobním datům zadávala minimálně 2 různá hesla)
* jakýkoliv systém by měl umožnit změnu hesla ze strany uživatele v jakýkoliv okamžik

3/ Aktualizace softwaru

* na počítačích je potřeba mít nainstalované pouze legální verze veškerého softwaru
* je nutné vždy mít software aktualizovaný, zejména
  + operační systém (aktualizuje se většinou automaticky)
  + kancelářský software, např. MS Office (aktualizuje se rovněž automaticky)
  + antivirový program a firewall
  + webový prohlížeč
  + software používaný pro práci s osobními údaji

4/ Předávání / zasílání osobních údajů

* osobní údaje předávané / zasílané v elektronické podobě by měly být vždy zabezpečené / zaheslované tak, aby v případě ztráty média (např. flash-disk) nebo nabourání se do emailu nebylo možné se k osobním údajům dostat bez znalosti přístupového hesla
* osobní údaje nelze posílat přímo v těle emailu / zprávy, ale formou zaheslované přílohy
* nejlépe je zasílat osobní údaje formou datové schránky

5/ bezdrátová síť - wifi

* nedoporučujeme používat wifi zcela nezabezpečenou / bez hesla
* minimální způsob zabezpečení je přístup do zabezpečené sítě přes heslo, které je dostupné pouze zaměstnancům a žákům školy
* heslo by se mělo pravidelně měnit - minimálně 1x ročně

6/ správa počítačové sítě

* podle rozsahu počítačové sítě by měla škola zajistit dostatečně kvalitní správu sítě tak, aby byly zajištěny potřebné činnosti (správa a nastavení uživatelských účtů, aktualizace softwaru, nastavení serveru apod.)

**Zpracovala**: Mgr. Pavla Marková, MBA, pověřenec pro ochranu osobních údajů na **Lepařovo gymnázium, Jičín, Jiráskova 30**

**Dne**: 9.5.2018