Posouzení vlivu používání scanu otisku prstu žáků ke vstupu do budovy základní školy

Správce : **Základní škola Dubá**

|  |  |
| --- | --- |
| se sídlem | : Dlouhá 113, 471 41 Dubá |
| IČO | : 48282979 |
| telefon | : ​ ​+420 487 883 951 |
| email | : ​skalicka@zsduba.cz |

**Cíl zamýšleného zpracování**

Škola má za povinnost zajistit přístup do budovy školy (prostoru šaten) pouze osobám, které mají oprávněný důvod do budovy vstupovat. V tomto případě se jedná o povolení vstupu žáků do budovy školy a prostorů šaten. Škola se snaží vyhnout vydávání, evidenci a řešení ztrát klíčů, magnetických vstupních karet nebo čipů. Škola se tedy již v minulosti a na základě doporučení a vyjádření dodavatele rozhodla pro toto řešení.

**Vhodnost použitého řešení :**  
Při použití tohoto řešení subjekt osobních údajů (žák) poskytuje biometrické osobní údaje formou scanu otisku prstu.  
Poskytnuté osobní údaje mají zajistit přístup žáků do šatních prostor školy vstupem pro žáky bez používání klíče nebo magnetického média typu čipu či magnetické karty.   
Čtecí zařízení pouze na základě přiložení prstu ke čtečce otevře žákovi vstupní dveře. Čtečka nezaznamenává žádné další údaje: např. identifikaci žáka a čas vstupu.   
Jednoduše lze říci, že celá aplikace slouží jako klíč ke vstupu žáků do školy.

**Potřebnost použitého řešení :**Přístup žáků do prostoru šaten bez zpracování jejich osobních údajů umožňují mj. tato řešení :   
- otevírání dveří pracovníkem školy;  
- instalace elektronického vrátníku s kamerou s tím, že vlastní vpuštění (po ověření žáka na monitoru) by opět zajistil pracovník školy;  
- vydávání klíčů, čipů nebo magnetických karet žákům.  
Jestliže by správce měl zajistit přístup žáků (otevření dveří) do prostor šaten jiným způsobem, než-li je scan otisku prstu, bude tento způsob vždy buď vyžadovat přítomnost pracovníka, který zajistí otevření dveří a vstup žáků do budovy školy, nebo bude muset zajistit výrobu, evidenci vydaných, vrácených a ztracených klíčů, magnetických karet nebo čipů.  
Řešení otevírání dveří do prostor šaten bylo správcem zvoleno s ohledem na požadavek minimalizace nákladů na pracovní síly.   
Řešení bylo v době instalace (před platností Nařízení GDPR) doporučeno dodavatelem včetně tohoto vyjádření :  
**Ochrana osobních údajů** při použití biometrické identifikace v systému Suprema platí, že § 4 písm. a) zákona č. 101/2000 Sb. stanoví, že o osobní údaj se nejedná, pokud je ke zjištění identity subjektu údajů třeba nepřiměřeného množství času, úsilí či materiálních prostředků. Za podmínky, že k otiskům prstů nejsou připojeny jiné údaje identifikující fyzickou osobu, že jsou uchovány v digitální podobě bez možnosti rekonstrukce do grafické podoby a bez možnosti využití pro jiné účely, nejsou otisky prstů osobními údaji.

Otisky prstů, které jsou pořízeny za účelem identifikace osob pro potřeby evidence docházky, kontroly vstupu a jiných podobných činností jsou v systému Suprema uloženy vždy jako binární šablony, ze kterých nelze zpětně rekonstruovat původní obraz otisku.

Vzhledem k výše uvedenému, je takovéto použití biometrických informací bezpečné a není v rozporu se zákonem č. 101/2000 Sb., o ochraně osobních údajů.

**Přiměřenost :**  
Správce považuje řešení založené na scanu otisku prstů za nejlépe vyhovující jeho potřebám a ve zvýšené míře neohrožující práva subjektu, pokud bude zajištěna dostatečná ochrana poskytnutých údajů (nepracuje se přímo s  biometrií prstu, ale s uloženým scanem otisku prstu, seznamem scanů otisku prstů a bezpečnou komunikací technických zařízení, není použita identifikace jméno a příjmení, ale pouze číselný identifikátor), dále pokud bude zajištěna možnost alternativního vstupu žáka do školní budovy při odmítnutí zpracování scanu otisku prstu zákonným zástupcem a pokud budou dostatečně a srozumitelně informováni žáci i jejich zákonní zástupci.

**Vlastnosti řešení SUPREMA BioStar**Čtecí zařízení i software pro správu je řešením dodávaným firmou SUPREMA s označením BioStar. Podle informací od dodavatele je toto řešení nastavitelné na různou úroveň zabezpečení a lze prohlásit, že je zajištěna :  
**Bezpečná ochrana biometrických dat pro šablony (scany otisků)**  
Reálné obrazy otisků prstů jsou ukládány jako šablony šifrované pomocí AES 128 nebo 256 bit případně DES nebo 3DES podle uložení šablony.  
**Ochrana osobních údajů uložených v databázi**  
Uložené osobní údaje v databázi mohou být šifrovány. Šifrování lze spustit v nastavení , které umožňuje klientské rozhraní.   
**Ochrana proti narušení transakcí**  
Ochrana komunikace pomocí šifrování a certifikátu se vztahuje na veškerou komunikaci TCP a RS-32, která se v systému používá. Komunikace je chráněna protokolem TLS 1.2 a komunikace mezi zařízeními je chráněna certifikátem.   
**Fyzická ochrana zařízení na čtečce (vstupním zařízení systému)**  
Zařízení mají bezpečnostní funkci, která chrání fyzická data ve čtečce tak, že pokud je neautorizovaná osoba odstraní ze zdi , všechna data uložená v zařízení (informace o uživateli, protokol událostí a šablony) budou vymazána a nastavení čtečky bude resetováno. Pokud je nastaveno šifrování osobních údajů v databázi, potom i data uložená ve čtečce jsou šifrována.   
**Protokoly**  
Systém je schopen vytvářet systémové protokoly, které zaznamenávají akce spojené s údržbou a instalací systému.  
Je možné nastavit automatické odstraňování protokolů po zvolené době.  
**Nastavení účtů**  
Lze nastavit různou úroveň pro přístup k datům pomocí práv pro jednotlivé uživatele (správce IT, bezpečnostní manager apod.)

**Instalace a nastavené pracovní postupy  
I. Počet instalovaných čteček**

|  |  |
| --- | --- |
| **Čtečka (ks)** | **Prostory instalace** |
| 1 | I.NP budovy školy. Venkovní strana dveří do prostoru šaten. Při vchodu ze dvora školy. |

**II. Instalovaný software:**

|  |  |
| --- | --- |
| **Zařízení** | **Prostory instalace** |
| server | I.NP. budovy v “serverovně“. Uložena šifrovaná databáze scanů otisků prstu. |
| PC | II.NP. budovy školy. Kancelář zástupkyně ředitelky.  Software (klientské řešení):  1. Připojení snímače otisků (“nahrávání“ nových nebo aktualizace stávajících).  2. Aktualizace databáze scanu otisků prstu (číselný identifikátor žáka a scan).  3.Spuštění exportu databáze scanu otisků prstu do čtečky u dveří. Do čtečky se exportuje pouze “seznam“ scanů. |

**III. Popis a umístění zařízení :**  
Čtečka je umístěna u vstupních dveří do prostoru šaten školy.  
Serverovna je uzamykatelná místnost s omezeným přístupem osoby. Přístup má koordinátor ICT (tedy zaměstnanec školy) a ředitelka školy. Přístup jiné osoby je umožněn pouze s doprovodem a s dohledem koordinátora ICT nebo ředitelky školy.   
Přístup k serveru a instalovaným aplikacím je chráněn heslem.  
Snímač prvotních otisků prstů žáků je uložen v uzamykatelné skříni a uzamykatelné kanceláři zástupkyně ředitelky. Software je instalovaný na počítači zástupkyně ředitelky, který je umístěn také v její kanceláři a zajištěn heslem při spuštění počítače (operačního systému Windows) a heslem při spuštění aplikačního software.

**IV. Proces snímání otisků**   
Na začátku školního roku provede zástupkyně ředitelky snímání otisku prstů nových žáků.  
V databázi na serveru jsou uloženy scany (šablony) otisky prstů žáků se jménem a číselný identifikátor žáka (žádné další osobní údaje nejsou zpracovávány).   
Provede se přenos scanu otisku prstů do čtečky u dveří.

**V. Přístupy**   
Osoba odpovědná za zpracování je zástupkyně ředitelky.   
Technická správa zařízení je zajištěna externí firmou smluvním vztahem.  
Existuje logování přístupů údržby.

**Posouzení zpracování scanu otisku prstů podle seznamu kritérií zpracování – hodnocení rizikovosti**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Pořadí*** | ***Kritérium*** | ***Hodnocení úrovně charakteristiky*** | ***Popis*** |
| *1* | *Zpracování zahrnující monitorování subjektů údajů.* | ***3*** | SUBJEKTY ÚDAJŮ JSOU IDENTIFIKOVATELNÉ/IDENTIFIKOVANÉ A JINAK MONITOROVANÉ. |
| *2* | *Zpracování kritických údajů, údajů umožňujících přímou identifikaci nebo údajů vysoce osobní povahy subjektů údajů.* | ***1*** | KRITICKÉ ÚDAJE – šablona (scan) otisku prstů a číselný identifikátor žáka uložený v databázi na PC zástupkyně a serveru. |
| *3* | *Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí.* | ***2*** | OMEZENÁ ZRANITELNOST  - subjekty jsou zařaditelné jako žáci. |
| *4* | *Zpracování osobních údajů velkého rozsahu.* | ***3*** | ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ MALÉHO ROZSAHU -  počet dotčených subjektů údajů je do 300. |
| *5* | *Zpracování zahrnující snímání veřejně přístupných prostor.* | ***3*** | PODROBNÁ ÚROVEŇ – MÍSTA VEŘEJNĚ OMEZENĚ PŘÍSTUPNÁ NEBO NEPŘÍSTUPNÁ. |
| *6* | *Zpracování osobních údajů s omezeným ovlivněním subjekty údajů.* | ***3*** | SUBJEKTEM ÚDAJŮ OVLIVNITELNÉ ZPRACOVÁNÍ NEBO PŘEDÁNÍ – zpracování má zákonný zástupce subjektu údajů možnost ovlivnit odvoláním souhlasu. |
| *7* | *Zpracování osobních údajů veřejn*ě *přístupných.* | ***3*** | ÚDAJE NEJSOU VEŘEJNĚ PŘÍSTUPNÉ. |
| *8* | *Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách či platformách.* | ***3*** | JEDNODUCHÝ SYSTÉM BEZ PROPOJENÍ NA JINÁ ZPRACOVÁNÍ. |
| *9* | *Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele.* | ***3*** | BEZ VAZEB NA JINÉ  SPRÁVCE NEBO  ZPRACOVATELE. |
| *10* | *Zpracování osobních údaj*ů *s využitím nových technologických či organizačních řešení.* | ***3*** | JDE O OPAKOVANÉ ŘEŠENÍ  NABÍZENÉ NA TRHU DODAVATELEM. |

**Vyhodnocení :**

|  |  |  |
| --- | --- | --- |
| **Úroveň charakteristiky** | **Popis** | **Počet** |
| 1 | KRITICKÉ HODNOTY | 1 |
| 2 | VÝZNAMNÉ HODNOTY | 1 |
| 3 | NÍZKÉ HODNOTY | 8 |

Vzhledem k tomu, že jedna úroveň charakteristiky dosáhla hodnoty kritické , ale současně pouze jedna úroveň dosáhla ​významné hodnoty, **není potřeba zpracovat DPIA charakteristiku​**.

**Účelem zpracování je**

zajistit žákům vstup do budovy školy-šaten při minimálních požadavcích na personální, technické a organizační zajištění tohoto procesu (evidenci vydaných, vrácených a ztracených klíčů nebo magnetických karet nebo čipů) , tím i minimálních nákladech na provoz.

**Právní základ pro zpracování​**

Zpracování probíhá podle čl. 6 odst. 1 písm. a) Nařízení GDPR, kdy zákonný zástupce udělil souhlas se zpracováním osobních údajů subjektu údajů (žáka). Zpracování osobních údajů tedy probíhá na základě **souhlasu se zpracováním osobních údajů.**Souhlas je vydáván na dobu docházky žáka do školy nebo do odvolání souhlasu zákonným zástupcem.  
Při odmítnutí souhlasu se zpracováním osobních údajů žáka bude tento žák vstupovat do budovy hlavním vchodem.

**Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu**

Danému účelu, tj. zajistit vstup žáků do prostorů šaten, je scan otisku prstu vhodný a s ohledem na účel. Při zajištění bezpečnosti databáze scanů otisku prstů a bezpečnosti údajů uložených ve snímači otisku prstů, při zajištění vhodných organizačních opatření a při současném nezbytném souhlasu zákonných zástupců lze zpracování scanů otisku prstů žáků považovat za přijatelné řešení.

**Posouzení rizik pro práva a svobody subjektů údajů**

Práva a svobody dotčených subjektů údajů mohou být narušeny v případě ztráty nebo odcizení přístupových hesel k počítači, k vlastní aplikaci zástupkyně ředitelky nebo ztráty či odcizení přístupových hesel k serveru. Následně pak odcizením databáze scanů otisku prstů ze serveru a jeho dešifrováním nebo odcizením čtečky otisku prstů s tím, že by došlo k selhání mechanismu, který při jakékoliv manipulaci se zařízením způsobuje její reset a vymazání uložených údajů.

Scan otisku prstu slouží výhradně k účelu výše uvedenému, není využíván k jakémukoliv sledování pohybu osob, jejich chování, jejich systematické identifikaci, kategorizaci či jinému profilování.

Níže popsaná plánovaná opatření vytvářejí akceptovatelnou míru rizika ohrožení práv a svobod subjektů.

**Plánovaná opatření k řešení rizik**

Scan otisku prstu slouží výhradně k účelu výše uvedenému, není využíván k jakémukoliv sledování pohybu osob, jejich chování, jejich systematické identifikaci, kategorizaci či jinému profilování.

Přístup ke scanu otisku prstů je možný pouze z uzamykatelných prostor. Případný nutný přístup jiné osoby je pod dozorem.  
  
Přístup k aplikaci, PC, kde je nainstalován software clienta a přístup k serveru má pouze omezený a určený počet osob (ředitelka školy, zástupkyně ředitelky, koordinátor ICT, správce serveru).

Počet osob s přístupem k databázi a software je omezen (ředitelka školy, zástupkyně ředitelky, správce serveru). Omezení se týká jak počtu osob, tak i situací, za kterých je možné k databázi a software přistupovat.

Přístup k serveru, databázi, clientské aplikaci na PC a všem používaným software je zabezpečen   
přístupovými právy.

Osobní údaje uložené v databázi jsou šifrovány (klíč 256 bit).

Scan otisku prstů je ukládán jako šablona šifrovaná pomocí AES 128 nebo 256 bit případně DES nebo 3DES podle uložení šablony.

Data exportovaná a uložená ve čtečce jsou šifrována.  
  
Čtečka má vlastní ochranu při násilné manipulaci (provede se reset čtečky a odstranění uložených údajů)

Servisní zásahy technika jsou prováděny tak, aby byl pod nepřetržitým dohledem koordinátora ICT, ředitelky nebo zástupkyně ředitelky.

Přístupy k serveru jsou logovány.

Přístupy k databázi scanu otisku prstů jsou logovány.

Zaměstnanci školy jsou vždy se systémem scanu otisku prstu při vstupu do prostor šaten seznámeni na začátku školního roku zástupkyní ředitelky.

Žáci školy jsou o způsobu použití systému scanu otisku prstu informováni učiteli. Tento soubor informací je předáván ústně na počátku každého nového školního roku.

Rodiče jsou o způsobu použití systému scanu otisku prstu informováni při podpisu souhlasu se zpracováním otisku prstu žáka jak ústně, tak i textem dokumentu souhlasu.   
U rodičů nových žáků se tak stává při zápisu do školy. Rodiče ostatních žáků jsou na probíhající zpracování upozorněni vždy na první rodičovské schůzce.

V Dubé 01.2.2021 ………………………………………………

Ing. Luděk Galbavý, LL.M