

Docházkové systémy a zpracování osobních údajů

V tomto dokumentu najdete informace o tom, jak námi dodávané docházkové čtečky DSi 800/700/502/501/500, přístupové terminály PSi 50/ACi, stravovací systémy SSi a stolní identifikátory pracují s otisky prstů a jakým způsobem dochází k jejich zpracování.

Pokud se rozhodnete používat otisky prstů a využívat je při vašem provozu pomocí námi dodávaných hardwarových řešení a dále v našich informačních systémech, tak při jejich používání nedochází k uchovávání úplných biometrických údajů. Při zpracování otisku prstu dochází pouze k výběru některých rysů specifických pro daný otisk a daného jednotlivce, ze kterých je vytvořena biometrická šablona. Tímto dojde k redukci úplného biometrického obrazu (tj. otisku prstu) s tím, že před uložením do systému je tato šablona dále ještě zpracována matematickými operacemi (tzv. hashováním) tak, aby nebyla volně čitelná nebo zpětně rekonstruovatelná, a to ani z části. Samotné hashe jsou pak drženy ve čtečce samotné a zkopírovány do cloudu, kde jsou poté zálohovány, a to přímo v databázi vaší společnosti. Každý jednotlivý otisk (nebo všechny otisky) pak můžete z cloudu snadno smazat, kdykoliv uznáte za vhodné, přičemž tímto bude také ihned odstraněn ze všech čteček.

O výše zmíněná technická řešení se staráme na naší straně, ale i přesto vyžaduje používání technologie zpracování otisků prstu pečlivý přístup také z vaší strany, protože dochází ke zpracování osobních údajů, které jsou současně biometrickými údaji dle čl. 4 bod 14) Obecného nařízení o ochraně osobních údajů Nařízení (EU) 2016/679 (dále jako „GDPR“). Nařízení GDPR spolu se zákonem č. 110/2019 Sb., o zpracování osobních údajů (dále jako „zákon o zpracování OÚ“), totiž klade na zpracovávání takových údajů (mj. dle čl. 9 odst. 1 GDPR se totiž jedná o tzv. zvláštní kategorii osobních údajů) zvýšené nároky.

Pro optimální používání našich hardwarových řešení je tedy třeba pečlivě zvážit a posoudit přiměřenost konkrétního řešení a rizika s ním spojená. Praxe se totiž posunula a při zpracovávání biometrických údajů, ať už je založené na principu identifikace (jedná se o situaci, kdy systém rozpoznává jednotlivce odlišením od ostatních osob, tzn. porovnáním údajů 1:N) nebo na principu autentizace (dochází pouze k ověření totožnosti fyzické osoby porovnáním údajů 1:1), je třeba pečlivě informovat každého, jehož biometrické údaje se chystáte zpracovávat a většinou také získat od všech dotčených fyzických osob souhlas se zpracováním jejich osobních údajů.

Naše hardwarová řešení umožňují využití otisků prstů nebo využití čipů a je pouze na vás, jak se rozhodnete s nimi pracovat. Měli byste však mít na paměti, že vaše rozhodnutí bude mít dopad na to, za jakých právních podmínek je možné systém využívat.

stojíme při Váš

Naše hardwarová řešení můžete využívat následovně:

1. Využití otisků prstů (identifikace) nebo kombinace čip+otisk prstu (autentizace)

Pokud chcete použít otisky prstů v zaměstnaneckých vztazích (např. k evidenci docházky), tak tento postup odpovídá systému identifikace nebo autentizace, což znamená, že při něm dochází ke zpracovávání zvláštních kategorií osobních údajů, na které se vztahuje přísnější režim čl. 9 GDPR. Zpravidla se tedy neobejdete bez výslovného svobodného, informovaného a zdokumentovaného souhlasu dotčených fyzických osob.

U zaměstnanců navíc platí specifické nároky, co se podmínek udělování souhlasu týká, a zaměstnavatel by měl být mj. vždy schopen doložit, že souhlas byl, i přes podřízené postavení zaměstnance, udělen skutečně svobodně. To ve zkratce znamená, že zaměstnanci musí být nabídnuta alternativa, kterou u našich čteček a systémů může být možnost využití čipu.

2. Využití čipů

Pokud se rozhodnete používat pouze čipy, tak v tomto případě nebude docházet ke zpracovávání jakýchkoli biometrických údajů a je tak možné činit bez jakéhokoliv souhlasu dotčené fyzické osoby, které bude čip vydán.

Možnost, kterou si zvolíte, můžete nastavit přímo na čtečce nebo v programu pro každého zaměstnance zvlášť. Všechna výše uvedená hardwarová řešení v sobě mají tuto funkčnost již od začátku a není nutné je nijak aktualizovat.

Obecně je potřeba uvést, že ať se již rozhodnete pro jakýkoliv způsob evidence docházky (tzn. i bez využití našich produktů), vždy se bude jednat o zpracovávání osobních údajů, u něhož bude nutné splnit nároky kladené GDPR a zákonem o zpracování.

Vnímejte, prosím, výše uvedené informace jako obecné shrnutí současné praxe, což však neznamená, že je možné se jimi bez dalšího řídit. Každé nakládání s osobními údaji je třeba vždy posoudit na konkrétních příkladech a v konkrétních podmínkách každého z vás.

Poslední revize 21.12.2022

stojíme při Váš