Zabezpečení biometrických údajů

Uchovávání biometrických údajů musí být zajištěno tak, aby byly maximálně omezeny možnosti jejich zneužívání. Do kategorie zneužívání patří jakékoli využívání mimo důvody, pro které byly biometrické údaje pořízeny, a které byly výslovně uvedeny v souhlasu, který subjekt udělil.

Šifrování

Uložené údaje musí být uchovávány šifrované tak, aby nebyly využitelné bez znalosti nebo nástroje, který není spolu s údaji dostupný. Pro autentizaci jsou uchovávány biometrické šablony. Ty by měly být uchovávány tak, aby z nich nebylo možné zpětně získat ucelený biometrický údaj nebo jeho podstatnou část (tzv. hash). I hash musí být uchováván jako osobní údaj s dostatečnou mírou ochrany.

Minimalizace kopií

Biometrické údaje mohou být zpracovány výhradně za účelem, ke kterému byly pořízeny. Proto mohou být uloženy pouze v místě (typicky v systému), který je zpracovává a nesmí být sdíleny s jinými systémy. Konkrétně nesmí být do jiných míst přenášeny nebo jiným systémům umožněno, aby biometrické údaje využívaly, nebo využívaly služby systému, který data zpracovává a který je pro služby poskytnuté jiným systémům využije.

Příklady:

- *Fakulta má fotografii studenta pořízenou za účelem vytvoření přístupové karty na pracoviště. (Pozor: Pro uchovávání musí mít svobodný souhlas, který uchovávání uvádí) Tuto fotografii nesmí pracoviště poskytnout jinému pracovišti k žádnému účelu.*
- *Systém fakulty uchovává šablonu biometrického podpisu používaného pro ověření dokumentu. Tento systém nesmí nabízet službu ověření biometrického podpisu jiným systémům (např. na jiných fakultách), pokud výslovnou součástí souhlasu nebylo sdílení tohoto údaje mezi fakultami.*
- *Docházkový systém uchovává hashe otisků prstů. Tento hash nesmí být součástí dat, které docházkový systém sdílí s jinými systémy, a to ani v případě, že by tyto jiné systémy hash nevyužívaly.*

Logování přístupů

Pokud jsou někde uchovávány biometrické údaje, musí být veškeré přístupy k místu jejich uložení logovány.

Příklady:

- *Pokud jsou uloženy někde např. fotokopie osobních dokladů, musí být každý konkrétní přístup k nim zaznamenán. Není proto např. možné, aby fotokopie dokladu byla v papírové složce v zamčené skříni, jejíž klíč je pracovníkům pracoviště dostupný. (Upozornění: Pro fotokopii musí být doložitelný také výslovný souhlas).*
- *Pokud je kopie vlastnoručního podpisu součástí smlouvy, smlouva nesmí být zveřejněna na internetu, ani nesmí být volně přístupná v rámci interního informačního systému tak, aby k její fotokopii s podpisem měli přístup pracovníci, kteří nepotřebují autentizovat podepisující osobu.*

Zabezpečení ve výzkumu vedeného více pracovišti

Pokud jsou biometrické údaje zpracovávány v rámci výzkumu více pracovišť, vždy musí být maximálně uplatněna možnost jejich anonymizace před předáním jinému pracovišti.

Příklady:

- *Nemocnice sbírá osobní údaje i biometrická data o pacientech na základě souhlasu o zapojení do výzkumu. Data jsou analyzována na pracovišti UK. Toto pracoviště přímo osoby nekontaktuje a nepotřebuje proto znát identifikační údaje osob, kterých se data týkají. Osobní údaje včetně biometrických jsou proto vždy předávány anonymizované.*
- *Pokud jsou předávány opakovaně údaje o stejných pacientech, jsou anonymizovány tak, aby pracoviště mohlo sledovat, které vzory patří ke stejné osobě, ale přesto není důvod, aby znalo jejich identitu.*

Je-li nezbytné, aby pracovníci různých pracovišť spolupracovali na využívání osobních údajů včetně biometrických dat, mělo by být využito vzdáleného přístupu ke sdílenému úložišti spravovaného jednou organizací, aby byla dodržena zásada minimalizace dat i jejich kopií.

Úroveň zabezpečení vzdáleného přístupu musí být adekvátní citlivosti zpracovávaných údajů a požadavků na ověření přistupujících osob, logování jejich přístupů a dokumentace důvodů, proč se k biometrickým údajům přistupovalo. Doporučeným postupem zabezpečení jsou osobní certifikáty členů týmu nebo dvoufaktorová autentizace.