Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7, Tel.: 234 665 111, Fax: 234 665 444; e-mail: posta@uoou.cz

STANOVISKO č. 3/2009

květen 2009

Biometrická identifikace nebo autentizace zaměstnanců

Úvod

Záměrem stanoviska je vyjádřit základní přístupy Úřadu pro ochranu osobních údajů (dále jen „Úřad“) pro použití systémů umožňujících spolehlivé určení fyzické osoby na základě unikátních biometrických znaků, které se v poslední době velmi rozšířilo i v pracovněprávních vztazích. Nejčastěji je ze strany zaměstnavatele vznášen požadavek na poskytnutí otisků prstů (případně otisku dlaně) zaměstnanců pro použití v přístupových a docházkových systémech. Použití biometrických znaků má vyloučit možnosti klamání zaměstnavatele při použití jiných prostředků, např. identifikačních karet, v docházkových systémech. V přístupových systémech má otisk prstu zajistit spolehlivé určení osoby oprávněné pro přístup do chráněných prostor nebo k chráněným informacím.

Otiskem prstu se rozumí obraz papilárních linií prstu včetně charakteristických změn (markantů) zaznamenaný na vhodném nosiči a určený pro další použití. V systémech biometrické identifikace nebo autentizace se markanty digitálně vyhodnocují. Systémy se mohou lišit počtem případně i druhem používaných markantů. Otisk prstu je považován za prakticky unikátní. To zakládá možnost přímého ztotožnění nositele zobrazované biometrické charakteristiky. Tím otisk prstu naplňuje znaky citlivého biometrického údaje jako údaje umožňujícího přímou identifikaci nebo autentizaci subjektu údajů podle § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Jakkoliv Úřadu přísluší posuzovat pouze operace prováděné s osobními údaji ve smyslu definice zpracování osobních údajů podle § 4 písm. e) zákona o ochraně osobních údajů, je třeba konstatovat, že i jiný požadavek na poskytnutí otisku prstu, než je shromažďování osobních údajů ve smyslu § 4 písm. f) citovaného zákona, představuje zásah do osobní integrity fyzické osoby, o jehož oprávněnosti by v případě sporu musel rozhodovat soud.

Odůvodnění

Záměr zaměstnavatele na trvalé ukládání biometrických údajů, například samotných scanů či snímků otisků prstů, často zpracovávaných společně s dalšími identifikačními údaji zaměstnanců v informačním systému zaměstnavatele v podobě, která umožňuje tyto informace dále zpracovávat, je zpracováním citlivých údajů, které je možné **jen za podmínek stanovených § 9 zákona o ochraně osobních údajů**, tedy buď s výslovným souhlasem subjektu údajů podle § 9 písm. a), nebo bez tohoto souhlasu za podmínek dále tímto ustanovením stanovených.

Přístupové systémy

Pokud se jedná o možnosti využití výjimky v § 9 písm. b) až i) zákona o ochraně osobních údajů pro zpracovávání biometrických údajů zaměstnanců, dá se využít toto ustanovení jen velmi omezeně. Z hlediska zákona o ochraně osobních údajů jde v tomto případě zejména o zpracování citlivých údajů, které je nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem ve smyslu § 9 písm. d), a dále se může jednat o zpracování nezbytné pro zajištění a uplatnění právních nároků ve smyslu § 9 písm. h), když tato možnost vyplývá ze zvláštních právních předpisů.

Z hlediska objektové bezpečnosti stanoví použití biometrické identifikace výslovně pouze vyhláška č. 144/1997 Sb., o fyzické ochraně jaderných materiálů a jaderných zařízení a o jejich zařazování do jednotlivých kategorií, vydaná k provedení zákona č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů. Tato vyhláška

v § 8 odst. 2 stanoví: „Každý, kdo je oprávněn vstupovat do střeženého, chráněného a vnitřního prostoru, je vybaven identifikační kartou umožňující automatickou kontrolu a registraci vstupu. Pro kontrolu vstupu osob se minimálně při vstupu do střeženého prostoru zařízení s jaderně energetickými reaktory použije biometrické identifikace (např. geometrie ruky, otisk prstů). Počet osob vstupujících do těchto prostorů se omezuje na nezbytně nutný počet. Aktuální databáze vstupů je dostupná jeden měsíc a zajišťuje se její archivace jeden rok."

Použití systémů využívajících biometrických znaků, které však nemusejí být založeny na vyhledávání biometrických údajů v databázi za tímto účelem vytvořené, tedy zpracování citlivých údajů ve smyslu zákona o ochraně osobních údajů, může být důvodné i v jiných případech souvisejících s pracovněprávními vztahy. Může jít zejména o přístupové systémy používané z hlediska fyzické bezpečnosti podle § 24 – 33 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, jako technického prostředku pro kontrolu vstupu ve smyslu § 30 odst. 1 písm. b) tohoto zákona. Podrobnosti upravují vyhlášky Národního bezpečnostního úřadu (NBÚ).

V praxi však u přístupových systémů, kde zajištění bezpečnosti zpracováním citlivých biometrických údajů není stanoveno zvláštním zákonem nebo spojeno se zvláštním zákonem předvídanou prováděcí vyhláškou, **lze biometrické identifikace s vyhledáváním biometrických údajů v databázi použít jen s výslovným souhlasem jejich nositele** podle § 9 písm. a) zákona o ochraně osobních údajů. Současně musejí být dodrženy všechny ostatní povinnosti správce podle zákona o ochraně osobních údajů, zejména § 10. V přístupových systémech by v návaznosti na uvedené mělo vždy platit pravidlo, že jde o mimořádné opatření kdy, kromě ze zvláštního zákona vyplývající povinnosti zajistit bezpečnost přístupu, se zpravidla zpracovávají biometrické údaje omezeného okruhu oprávněných osob, na rozdíl od plošného zpracování biometrických údajů všech zaměstnanců v docházkových systémech.

Docházkové systémy

Podle přístupu Úřadu k této problematice deklarovaného ve výroční zprávě za rok 2007 i v odpovědích na četné dotazy veřejnosti k této problematice nelze použití systémů, v jejichž paměti dochází k uchovávání biometrických údajů v podobě, která umožňuje jejich další zpracování, považovat za nezbytné pro jakoukoliv běžnou evidenci, např. pro evidenci docházky do zaměstnání. Zpracování biometrických údajů zejména v docházkových systémech lze proto posuzovat jako nepřiměřené ve vztahu k rozsahu a účelu zpracovávání, který je povinen stanovit každý správce. V důsledku toho může docházet k porušení povinnosti podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, tedy shromažďování osobních údajů neodpovídajících stanovenému účelu a v rozsahu nikoli nezbytném pro naplnění stanoveného účelu, a to i v případě existence výslovného souhlasu subjektu údajů. Na takový postup zaměstnavatele lze podat Úřadu stížnost. Ani splnění oznamovací povinnosti správce podle § 16 problém zaměstnavatele neřeší, protože takové zpracování by nemohlo být ve smyslu § 17 odst. 2 povoleno. Obdobný přístup zaujímá většina úřadů na ochranu dat států Evropské unie.

Problematice zpracování biometrických dat se věnuje Pracovní dokument o biometrii, který 1. srpna 2003 přijala Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená v rámci Evropské komise podle článku 29 směrnice 95/46/ES Evropského parlamentu a Rady (Working Party - WP29).

Prvním podstatným hlediskem je, zda dochází k uchovávání úplných biometrických údajů, nebo zda systém vybírá z úplných biometrických údajů některé rysy specifické pro jednotlivce tak, aby vytvořil biometrickou šablonu, která je redukcí úplného biometrického obrazu.

Je žádoucí, aby šablony byly před uložením v systému zpracovávány matematickými operacemi (kódování, algoritmy nebo hash funkce) tak, aby nebyly volně čitelné nebo zpětně rekonstruovatelné.

Důležité přitom je, že různé systémy mají různé způsoby bezpečného převodu šablony otisku prstů do číselného vyjádření, které je uloženo v systému. Nelze proto říci, že určité takto získané číselné vyjádření je pro subjekt údajů ve všech systémech jednoznačné. Zpracování takovýchto číselných vyjádření šablon tedy nelze posuzovat jako zpracování biometrických údajů.

Jiná situace by ovšem nastala v případě, kdy by existoval pouze jediný způsob převodu, a tudíž by každý subjekt měl ve všech těchto systémech jedinou hodnotu.

Jestliže dojde např. při použití jednosměrného hashování k vytvoření číselného údaje, jehož zpětná rekonstrukce na biometrický údaj není možná, nelze již tento údaj považovat za biometrický a využití

takového systému může být v určitých případech přípustné, a to při naplnění povinností správce podle § 5 odst. 1 a dále některé z podmínek § 5 odst. 2 písm. a), b) nebo e) zákona o ochraně osobních údajů i bez souhlasu subjektu údajů, protože nedochází k uchovávání citlivého údaje.

Pro další zpracování údajů o docházce do zaměstnání za účelem plnění práv a povinností vyplývajících z pracovněprávních vztahů je v tom případě **aplikovatelná i výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů**. Další zpracování osobních údajů zaměstnance např. na základě osobního čísla zaměstnance již není zpracováním citlivých údajů. Podléhá proto ostatním povinnostem stanoveným zákonem o ochraně osobních údajů, se zákonem stanovenými výjimkami, ne však režimu § 9.

Dalším důležitým hlediskem je, zda je použitý systém založen na autentizaci (verifikaci) fyzické osoby, nebo na identifikaci subjektu údajů v databázi, v níž jsou uchovávány osobní údaje i dalších subjektů údajů. Autentizační (verifikační) systém pouze ověřuje totožnost fyzické osoby porovnáním údajů 1:1. Při identifikaci systém rozpoznává jednotlivce odlišením od ostatních osob, tedy výběrem jednoho z *n* možných případů.

Plné biometrické údaje nebo biometrické šablony tedy mohou být uchovávány buď pouze v paměti biometrického zařízení nebo v centrální databázi, případně u některých systémů na optických, nebo čipových kartách, které uživatelům umožňují nosit je při sobě jako identifikační prostředek.

Aplikace pro autentizaci (verifikaci) se často používají pro různé úkoly ve zcela odlišných oblastech a v odpovědnosti celé řady různých subjektů. Pro účely autentizace/verifikace není nezbytné uchovávat osobní údaje v databázi, postačuje je uchovávat decentralizovaně. Z hlediska zásady proporcionality jsou jednoznačně upřednostňovány biometrické aplikace, které nezpracovávají data získaná z tělesných stop nevědomě zanechaných jednotlivci a u kterých nejsou data uchovávána v centralizovaném systému.

Povinnostem stanoveným zákonem o ochraně osobních údajů pro zpracování citlivých údajů proto nemusí podléhat systém, který pracuje pouze na principech autentizace, tedy metody kontroly příchodu a odchodu zaměstnance, kdy čtecí zařízení, do kterého otisk prstu vkládá na základě požadavku zaměstnavatele na kontrolu docházky sám zaměstnanec, porovnává údaje 1:1.

Při příchodu na pracoviště nebo odchodu z něj je po zvolení osobního čísla zaměstnance vložený otisk s přiložením příslušného prstu použit pouze pro ověření totožnosti subjektu údajů. Do dalšího zpracování osobních údajů snímek otisku prstu nebo dlaně však již nevstupuje a systém jeho další zpracování ani neumožňuje. Osobní číslo zaměstnance je v takovémto docházkovém systému druhým identifikátorem, který však může být zaměstnavatelem zpracováván v souladu se zákonem o ochraně osobních údajů i bez souhlasu subjektu údajů ve smyslu § 5 odst. 2 písm. e).

Rozhodné pro posouzení, zda jde o z hlediska zásad ochrany přípustnou autentizaci, nebo o identifikaci, kterou je třeba podrobit přísné regulaci je, zda účelem použití otisku prstu, je pouze ověření totožnosti porovnáním s přiloženým prstem ruky, nebo v systému dochází v návaznosti na přiložení ruky nebo její části (případně karty s RFID čipem, který již tyto informace obsahuje) k vyhledávání a porovnávání informací s údajem uchovávaným v databázi biometrických údajů, která musí být vždy považována za zpracování citlivých údajů, podléhající režimu § 9 zákona o ochraně osobních údajů.

I zde však platí, že pro další zpracování osobních údajů zaměstnanců mohou být uplatněny výjimky pro zpracování bez souhlasu subjektu údajů podle § 5 odst. 2 písm. a), b) nebo e) a výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b), ale je třeba upozornit, že Úřad bude aplikaci těchto výjimek u všech systémů založených na použití biometrických znaků posuzovat nadále velmi obezřetně.

Zaměstnavatel musí důsledně splnit nejen shora uvedené povinnosti podle § 5, 9 a 16, ale dále také informační povinnost podle § 11 a povinnosti při zabezpečení osobních údajů podle § 13 - 15 zákona o ochraně osobních údajů, jestliže by šlo o shromažďování citlivých údajů umožňující jejich další zpracování v databázi, ale v případě jakéhokoliv systému založeného na použití biometrických znaků i informační povinnost o základních pracovních podmínkách a jejich změnách podle § 279 zákoníku práce, neboť může nastat situace, kdy zaměstnanec výlučně vstupní otisk prstu pro ověření totožnosti neposkytne z obavy z jeho možného zneužití.

Závěr

Je třeba zdůraznit, že zejména **biometriku založenou na zpracování citlivých údajů v centrální databázi lze v pracovněprávních vztazích využívat jen ve výjimečných situacích.** Připomenout je třeba i povinnosti zaměstnavatele podle § 316 zákoníku práce, týkající se zákazu otevřeného i skrytého sledování zaměstnance. Toho by se zaměstnavatel mohl dopustit, pokud by pro kontrolu docházky přípustný systém biometrické autentizace využíval pro kontrolu pohybu zaměstnance na pracovišti nad rámec evidence přítomnosti zaměstnance na pracovišti podle § 96 odst. 1 písm. a) zákoníku práce.

Zaměstnancům, kteří mají pochybnosti o oprávněnosti požadavku zaměstnavatele na poskytnutí otisku prstu, Úřad doporučuje využít práva, které dává zákon o ochraně osobních údajů v § 21: Požádat zaměstnavatele o vysvětlení na jakém základě systém funguje. V případě, že by šlo o systém založený na zpracování biometrických údajů jejich vyhledáváním v databázi, nemusejí k tomu dávat souhlas a mohou se na Úřad obrátit s podnětem podle § 21 odst. 4 zákona o ochraně osobních údajů.