7. 7. 2017

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Zpracování biometrických údajů ve světle obecného nařízení o ochraně osobních údajů (GDPR)

Biometrickými údaji jsou takové informace, které vypovídají o jedinečných biologických charakteristikách člověka a odlišují jej od všech ostatních. V praxi jsou využívány biometrické údaje týkající se otisků prstů či dlaně, snímků oční rohovky, charakteristik rukopisného podpisu, ale i hlasu, chůze, snímku obličeje atd. S ohledem na to, že biometrické údaje jsou jedinečné a prakticky neměnné, týkají se tedy vždy konkrétní a jednoznačně určitelné osoby, je jejich shromažďování a další zpracování podřízeno pravidlům pro zpracování osobních údajů.

Právní úprava a dosavadní výklad Úřadu pro ochranu osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, pak, na rozdíl od Směrnice 95/46 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, kterou právě uvedený zákon transponuje do českého právního řádu, řadí biometrická data mezi citlivé údaje, tedy údaje, pro jejichž zpracování platí přísnější pravidla. Zařazení biometriky mezi citlivé údaje bylo provedeno tzv. euronovelou, tedy zákonem č. 439/2004 Sb.[1]

V praxi jsou biometrické údaje či systémy založené na zpracován biometriky typicky využívány pro evidenci docházky zaměstnanců, pro kontrolu vstupu na režimová pracoviště, jako bezpečnostní prvek pro přihlašování do prostředků výpočetní techniky (mobilní telefon, počítač) či v systémech pracujících s biometrickým podpisem. Zmíněný přísnější režim pro zpracování této kategorie údajů spočívá především v nutnosti disponovat některým ze specifických právních titulů pro zpracování citlivých údajů taxativně vypočtených v § 9 zákona č. 101/2000 Sb., protože právní tituly pro zpracování „běžných“ údajů, které jsou upraveny v § 5 odst. 2 téhož předpisu, na zpracování citlivých, biometrických údajů využít nelze. Jinak řečeno, zatímco běžné osobní údaje zpracovávané například za účelem evidence docházky, ověření identity či kontroly vstupu, lze obvykle zpracovávat bez souhlasu dotčených osob, jelikož se jedná o zpracování údajů nezbytné k ochraně práv či právem chráněných zájmů správce údajů či jiné osoby [právní titul dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.], v případě zpracování biometrických, tedy citlivých údajů, tento právní titul uplatnit nelze a správce ke zpracování biometrických údajů za těmito účely ve velké většině případů musí získat výslovný souhlas dotčených osob.[2]

Dozorový úřad, Úřad pro ochranu osobních údajů, k variantám využití biometrických údajů a jejich důsledku z pohledu výše zmíněné právní úpravy vydal v roce 2009 obecné výkladové stanovisko.[3] Podle tohoto stanoviska lze odlišit v zásadě dvě technická řešení s odlišnými právními důsledky.

Prvním je takové, kdy jsou biometrické údaje na vstupu pouze sejmuty a následně převedeny na číselnou řadu způsobem, který neumožňuje zpětnou rekonstrukci biometrických charakteristik. Při využívání systému tak nedochází k uchování ani k aktivnímu využívání biometriky při identifikaci či autentizaci. V takovém případě se dle názoru ÚOOÚ jedná o systém zpracovávající osobní, nikoliv citlivé údaje, a jeho provoz tudíž lze opřít i o jiné právní tituly, než je výslovný souhlas dotčených osob.

Do druhé kategorie pak předmětné stanovisko řadí systémy, které s biometrickými údaji aktivně pracují, např. při ověřování každého dalšího podpisu dané osoby, spuštění či aktivaci mobilního telefonu nebo počítače atd. Tyto systémy pak zpracovávají citlivé údaje ve smyslu zákona o ochraně osobních údajů a, až na malé výjimky, je pro jejich provoz nezbytné disponovat výslovným souhlasem osob, jejichž údaje jsou takto zpracovávány.

Nová právní úprava a změna výkladu dozorového úřadu

Dne 25. května 2018 nabývá v Evropské unii účinnosti Obecné nařízení o ochraně osobních údajů[4] (GDPR). Toto nařízení nahrazuje dosavadní směrnici 95/46/ES. Jednou ze změn oproti směrnici je zařazení biometrických údajů mezi zvláštní kategorii osobních údajů. Pro tyto kategorie osobních údajů obecně platí, že jejich zpracování se zakazuje. Z tohoto obecného zákazu pak existuje několik výjimek, kdy lze tyto údaje zpracovávat. Tyto výjimky, neboli právní tituly pro zpracování, jsou odlišné od těch uvedených v čl. 6 GDPR platící pro osobní údaje obecně. Lépe řečeno, možnosti zpracování zvláštních kategorií osobních údajů jsou oproti zpracování „běžných" osobních údajů omezenější.[5]

Zejména v souvislosti se zařazením biometrických údajů mezi zvláštní kategorie osobních údajů v GDPR Úřad pro ochranu osobních údajů uveřejnil informaci o změně v hodnocení úrovně právní ochrany biometrických údajů.[6] Dle postoje Úřadu pro ochranu osobních údajů se již do budoucna nebude rozlišovat mezi výše zmíněnými variantami technických řešení využívání biometrických údajů. Jakýkoliv systém, který shromažďuje biometrická data za účelem identifikace konkrétních osob bude považován za systém zpracovávající zvláštní kategorii osobních údajů. Pro obě výše popsané kategorie systémů tak budou platit stejná pravidla.

Co změna výkladu znamená pro praxi?

Ve světle tohoto posunu výkladu dozorového úřadu, Úřadu pro ochranu osobních údajů, tak dochází k rozšíření aplikace ustanovení o zpracování citlivých údajů (zvláštní kategorie osobních údajů dle GDPR) na další systémy. Změna se tak dotkne například výše zmíněných docházkových systémů zaměstnavatelů, které jenom převádějí otisk prstu do číselného vyjádření, které bylo pak uložené v systému. V praxi to bude pro zaměstnavatele i další správce znamenat nutnost zejména získat výslovný souhlas subjektu údajů ke zpracování biometrických údajů. V tomto případě není možné využít oprávněný zájem správce jako právní titul, jak je tomu například v rámci docházkových systému nezpracovávajících biometrická data. S ohledem na recitál 171 GDPR bude od účinnosti tohoto nařízení platný jen takový souhlas, který bude splňovat náležitosti této nové úpravy. Nelze tedy než doporučit, aby správce, který nyní začne shromažďovat souhlas se zpracováním biometrických či jiných citlivých osobních údajů, tak již činil způsobem a formou odpovídající požadavkům nového nařízení, aby jej nemusel po květnu příštího roku získávat znovu.

V souvislosti se zpracováváním biometrických údajů je důležité zdůraznit, že zpracovávání těchto údajů obvykle představuje vyšší riziko pro práva dotčených osob. Rizikovost zpracování je přitom faktorem, který je v rámci GDPR zohledňován na mnoha místech a který je nutný brát v potaz jak při stávajících způsobech zpracování, tak i při zavádění těch nových. Například pokud správce zpracovává biometrické údaje, měla by být tento fakt reflektován v zabezpečení, které využívá. Obecně platí, že biometrický údaj jako údaj spojený s vyšším rizikem pro subjekt údajů by měl být podroben vyšší úrovni zabezpečení.

Zpracování biometrický údajů bude mít dopad i na povinnost vypracovat Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment - DPIA). Povinnost vypracovat DPIA má správce v případě, že je pravděpodobné, že určitý druh zpracování bude s přihlédnutím k povaze, rozsahu,

kontextu a účelům mít za následek vysoké riziko pro práva a svobody fyzických osob.[7] Dle zveřejněné verze vodítka k posouzení vlivu na ochranu osobních údajů a návod pro hodnocení úrovně rizika zpracování pracovní skupiny WP29[8] představuje zpracování biometrický údajů jeden z důvodů pro vypracování DPIA.

Další dopad lze spatřovat i v rámci povinnosti ohlašování případů porušení zabezpečení osobních údajů. Tato nová povinnost zavedená GDPR dává správcům za úkol oznamovat Úřadu pro ochranu osobních údajů jakékoli porušení zabezpečení osobních údajů. Správce tuto povinnost nemusí plnit jenom v případě, kdy je nepravděpodobné, že by takové porušení mělo za následek riziko pro práva a svobody fyzických osob. V případě biometriky, jakožto kategorie osobních údajů podléhající zvýšené ochraně, nicméně nebude pravděpodobně možné tuto výjimku aplikovat. Navíc porušení zabezpečení biometrických údajů, zejména jejich únik, bude pro správce obvykle znamenat i povinnost oznámit toto porušení nejen Úřadu pro ochranu osobních údajů ale i samotnému subjektu údajů, jelikož v mnoha případech lze předpokládat, že porušení takových údajů bude mít za následek vysoké riziko pro fyzické osoby.[9] Zde lze správcům i zpracovatelům doporučit, jak již bylo naznačeno i výše, zvýšenou úroveň ochrany biometrických údajů, například v podobě šifrování těchto údajů, která může efektivně snížit daná rizika.[10]

Co naopak výše uvedená změna výkladu Úřadu pro ochranu osobních údajů neznamená? Podle názoru autorů ani s ohledem na změnu právní úpravy a související změnu výkladu dozorového úřadu nelze konstatovat, že by ke zpracování biometrických, či obecně citlivých osobních údajů, docházelo tehdy, když jsou tyto shromažďovány jako technicky nezbytná součást daného procesu, použité technologie, bez úmyslu biometrická data jakkoliv využívat či jinak zpracovávat. Příkladem může být kamera či fotografický přístroj, který již obvykle pořizuje záznamy či snímky v takové kvalitě, že z nich lze v řadě případů vyčíst biometrické markanty. Pokud provozovatel sledovacího systému tyto údaje shromažďuje neúmyslně, jako nedílnou součást shromažďování běžných identifikačních údajů (podoba člověka), a nijak s nimi dále nepracuje, i nadále platí, že se jedná o zpracování osobních, nikoliv citlivých osobních údajů.[11] Stejný přístup bude nadále aplikovatelný i ve vztahu k dalším informacím spadajícím do zvláštní kategorie osobních údajů, které sledovací systém jako nezbytnou součást pořizování záznamu zachycuje, typicky se jedná o údajů o etnickém či rasovém původu. Z tohoto úhlu pohledu změna právní úpravy a výkladu Úřadu pro ochranu osobních údajů praktické důsledky nemá.

Mgr. František Nonnemann

Mgr. Michaela Skácelová

Autoři jsou zaměstnanci MONETA Money Bank, a.s.
Článek vyjadřuje osobní názor autorů, nikoliv jejich zaměstnavatele.

---

[1] Srov. definiční ustanovení § 4 písm. b) zákona č. 101/2000 Sb. a čl. 8 směrnice 95/46/ES.
[2] Ve výjimečných případech je povinnost chránit vstup na některá režimová pracoviště i za využití biometriky stanoven přímo právním předpisem, srov. § 11 odst. 2 vyhlášky č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu.
[3] Stanovisko č. 3/2009, Biometrická identifikace nebo autentizace zaměstnanců, dostupné na www.uoou.cz. Stanovisko se sice zabývá využitím biometriky v pracovněprávní oblasti, nicméně jeho závěry je možné uplatnit obecně.

[4] Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[5] GDPR dává členským státům možnost rozšířit či omezit právní tituly pro zpracování biometrických údajů, takže je možné, že implementační zákon ke GDPR umožní zpracovávání biometriky nad rámec toho, co povoluje čl. 9.
[6] Informace ze dne 8.6.2017 dostupná na webových stránkách Úřadu pro ochranu osobních údajů zde https://www.uoou.cz/zmena-v-hodnoceni-urovne-pravni-ochrany-biometrickych-udaju/d-23850
[7] Čl. 35 odst. 1 GDPR
[8] Vodítka dostupné na webových stránkách Evropské Komise >>> zde
[9] Čl. 33 a 34 GDPR
[10] Více k aplikaci přístupu založenému na riziku (risk-based approach) srov. Nulíček, M. Donát, J. Nonnemann, F. Lichnovský, B. Tomíšek, J. GDPR. Obecné nařízneí o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017.
[11] Srov. Kučerová, A. a spol. Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2012.

Další články:

- Byznys a paragrafy, díl 32.: Konkurenční doložka
- Skryté ujednání v realitní smlouvě – zbytečná hra na schovávanou
- Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnické osobě
- Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu
- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše