EVERY REGARD s.r.o.
Zámostní 1155/27
Ostrava-Slezská Ostrava, 710 00
IČO: 05460034 – společnost není plátcem DPH

Zpracování biometrických údajů zaměstnanců

Podle nařízení EU č. 2016/679 o ochraně osobních údajů (GDPR) se biometrickými údaji rozumí osobní údaje týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují její jedinečnou identifikaci. Nejvíce se v praxi používají otisky prstů nebo dlaně, zobrazení obličeje, snímky oční rohovky, biometrický dynamický podpis nebo hlas. Zaměstnavatelé v rostoucí míře zpracovávají biometrické údaje zaměstnanců za účelem evidence docházky nebo kontroly vstupu na vybraná pracoviště anebo jako bezpečnostní opatření pro přihlášení do technických zařízení (např. počítač nebo telefon). Jelikož se biometrické údaje považují za osobní údaje zvláštní kategorie, tak jsou pro jejich zpracování stanovena přísná pravidla.

Současná právní úprava

Zpracování biometrických údajů nyní upravuje nařízení GDPR. Biometrické údaje patří mezi tzv. osobní údaje zvláštní kategorie, pro které platí obecný zákaz jejich zpracování. Nicméně článek 9 odst. 2 GDPR stanoví několik výjimek z tohoto zákazu, zejména v případě (a) výslovného souhlasu subjektu údajů; (b) plnění povinností správce údajů nebo subjektu údajů v oblasti pracovního práva a sociálního zabezpečení, pokud je povoleno právem EU nebo členského státu (např. předávání osobních údajů zaměstnavatelem zdravotní pojišťovně); (c) ochrany životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, pokud subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas; a další.

Navíc podle článku 9 odst. 4 nařízení GDPR členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu. Z tohoto ustanovení není zcela zřejmé, zda členské státy mohou tyto podmínky zpracování mj. biometrických údajů pouze zpřísnit nebo také zmírnit. Ovšem pravděpodobně bude přípustné tyto podmínky i zmírnit vzhledem ke znění ustanovení, vnitrostátní aplikaci jiných členských států a aktuálnímu výkladu Úřadu pro ochranu osobních údajů ČR (ÚOOÚ). V České republice zatím žádná zvláštní úprava ve vztahu ke zpracování biometrických údajů zaměstnanců údajů.

Úřad pro ochranu osobních údajů rozlišoval do účinnosti GDPR (tj. květen 2018) dva možné způsoby zpracování biometrických údajů s odlišnými právními režimy.[1]

1) Za první způsob ÚOOÓ označoval zpracování biometrických údajů (např. otisků prstů), při němž se uchovávají pouze některé znaky vytvářející redukovanou biometrickou šablonu (převedenou např. na číselný údaj), která není volně čitelná a není ji možné převést zpět na biometrický údaj. Při snímání biometrického obrazu tak dochází pouze k ověření totožnosti zaměstnance a samotné biometrické údaje nejsou dále zpracovány. Podle ÚOOÚ se v takovém případě nejednalo o zpracování citlivých osobních údajů, a tudíž nebyl nutný výslovný souhlas dotčených osob nebo jiný právní titul stanovený pro zpracování citlivých osobních údajů (resp. dle GDPR údajů zvláštní kategorie).

2) Do druhé skupiny zpracování biometrických údajů byly řazeny technická řešení, která biometrické údaje uchovávají a aktivně je využívají například pro verifikaci každého dalšího podpisu subjektu údajů a umožnují tedy další zpracování těchto biometrických údajů. Taková technická řešení posuzoval ÚOOÚ jako zpracování citlivých osobních údajů, která zásadně vyžadují výslovný souhlas subjektu údajů.

ÚOOÚ vydal v návaznosti na účinnost nařízení GDPR nové stanovisko upozorňující na změnu v jeho hodnocení právní ochrany biometrických údajů.[2] V tomto stanovisku se mj. uvádí, že uchování biometrických šablon a jejich zpracování za účelem identifikace osob se podle GDPR považuje za zpracování osobních údajů zvláštní kategorie. Podle ÚOOÚ tak není možné od účinnosti GDPR postupovat v mezích jeho dosavadního stanoviska k biometrickým údajům č. 3/2009. Z nového stanoviska ÚOOÚ vyplývá, byť ne zcela jasně, že jakékoliv zpracování biometrických údajů za účelem identifikace osob má být posouzeno jako zpracování osobních údajů zvláštní kategorie.
Oba výše uvedené způsoby zpracování biometrických údajů tedy podle ÚOOÚ vyžadují výslovný souhlas dotčených subjektů údajů nebo jiný právní titul stanovený v článku 9 odst. 2 nařízení GDPR.

Návrh ÚOOÚ na změnu právní úpravy v zákoníku práce
Pokud by se jakékoliv zpracování biometrických údajů řídilo pravidly GDPR pro zpracování osobních údajů zvláštní kategorie, tak dle stávajícího právního řádu ČR by zaměstnavatel zásadně nemohl zpracovávat biometrické údaje zaměstnanců bez jejich výslovného souhlasu. Výslovný souhlas však musí být kdykoliv odvolatelný. Zaměstnavatel by tudíž nemohl ani v odůvodněných případech kontrolovat docházku zaměstnanců nebo jejich přístup na pracoviště se zvláštním režimem na základě sejmutí otisku prstu nebo jiného biometrického údaje; až na výjimky jako je například kontrola vstupu do prostoru zařízení s jaderně energetickými reaktory, kdy zákon výslovně stanoví, že se použije biometrické identifikace.

> **S ohledem na výše uvedené ÚOOÚ podal připomínku k návrhu novely zákoníku práce předkládané Ministerstvem práce a sociálních věcí, v níž navrhuje řešení problematiky zpracování biometrických údajů.[3] Tato novela měla nabýt účinnosti k 1. červenci 2019 a částečně k 1. lednu 2020, avšak ještě nebyla předložena Poslanecké sněmovně, a proto lze očekávat posunutí účinnosti na pozdější termín. Novela zákoníku práce se dotýká mj. úpravy dovolené, dočasného přidělení a přechodu zaměstnanců, sdílených pracovních míst a doručování.**

ÚOOÚ navrhuje, aby v rámci této novely zákoníku práce bylo přijato nové ustanovení § 316a upravující biometriku zaměstnance. Systematicky by se tedy jednalo o doplnění stávajícího ustanovení § 316 zákoníku práce, které upravuje ochranu majetkových zájmů zaměstnavatele a ochranu osobních práv zaměstnance včetně podmínek, za kterých může zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele (sledováním zaměstnance, odposlechem záznamu jeho telefonických hovorů, kontrolou elektronické pošty či listovních zásilek). Zákoník práce nyní vyžaduje, aby zaměstnavatel měl k zavedení takových kontrolních mechanismů závažný důvod spočívající ve zvláštní povaze činnosti (např. nebezpečný provoz nebo i ochrana majetku) a aby zaměstnavatel informoval zaměstnance o rozsahu kontroly a způsobech jejího provádění.

Podle ÚOOÚ však současná právní úprava neobsahuje výslovné zmocnění ke zpracování biometrických údajů zaměstnavatele v souladu s GDPR, a proto neopravňuje zaměstnavatele ke zpracováním biometrických údajů zaměstnanců za účelem evidence docházky nebo kontroly vstupu na pracoviště.

Z tohoto důvodu ÚOOÚ navrhuje, aby zákoník práce výslovně stanovil, že zaměstnavatel může využívat k ochraně svých výrobních a pracovních prostředků a technologií biometrické údaje identifikující zaměstnance a používající pouze morfologické znaky zaměstnanců (např. digitální otisk, scan žilního systému ruky). Dle návrhu ÚOOÚ by tyto údaje bylo možné vyžívat výhradně pro účely kontroly přístupu k výrobním a jiným provozním zařízením zaměstnavatele a vstupu do objektů zaměstnavatele nebo jejich částí, kde jsou taková zařízení umístěna. Pro tyto účely a v přímé věcné souvislosti s nimi by se navíc mohly zpracovávat jen tyto údaje: (a) obecné identifikační údaje zaměstnance včetně fotografie a jeho identifikační údaje vytvořené zaměstnavatelem; (b) dále nezbytné provozní údaje (např. pracovní zařazení a přiznaná oprávnění) a (c) osobní údaje vytvořené technickým zařízením nebo za jeho pomoci, tj. zpravidla vstupy a přístupy.

Ostatní podmínky zpracování biometrických údajů zaměstnanců (zabezpečení údajů, ohlašování bezpečnostních incidentů, doba uchování údajů, informování a práva zaměstnanců jako subjektů údajů) by se pak řídily obecnými ustanoveními GDPR.

EVERY REGARD s.r.o.
Zámostní 1155/27
Ostrava-Slezská Ostrava, 710 00
IČO: 05460034 – společnost není plátcem DPH

RESUME.

1. Lze shrnout, že v případě biometrické docházky je jediným v úvahu připadajícím zákonným důvodem zpracování souhlas zaměstnance.
2. Nicméně souhlas musí být prokazatelně svobodný. Tento souhlas nesmí být dle obecně přijímaného výkladu součástí pracovní smlouvy.
3. Zaměstnavatel musí být schopen prokázat, že zaměstnanci měli při udělení na výběr, musel by tedy mít „v záloze“ i jinou možnost evidence docházky pro případ, kdy (někteří) zaměstnanci odmítnou souhlas udělit.
4. Přitom je nutno si uvědomit, že souhlas je vždy udělován jako kdykoli odvolatelný. Aby tedy zaměstnavatel minimalizoval rizika, musel by mít zavedeny dva systémy sledování docházky – jeden pro zaměstnance, kteří souhlasili s užitím biometrických údajů, a druhý pro zaměstnance, kteří souhlas neudělili, popř. jej odvolali.
5. Evidence docházky prostřednictvím biometrických údajů zaměstnance tedy není právně zcela vyloučena, je však otázkou, zda je takové řešení s ohledem na shora popsané limity pro zaměstnavatele výhodné a praktické.

Miroslav Kalinský
GDPR konzultant a DPO
V Ostravě dne 9. listopadu 2020

[1] Stanovisko ÚOOÚ č. 3/2009, Biometrická identifikace nebo autentizace zaměstnanců. K dispozici >>> **zde**:
[2] Stanovisko ÚOOÚ č. 1/2017. K dispozici >>> **zde**.
[3] Připomínka ÚOOÚ k návrhu novely zákoníku práce. K dispozici >>> **zde**.