

ZPRAVODAJ PRO MZDOVÉ ÚČETNÍ A PERSONALISTY

čtrnáctideník aktualit, komentářů a příkladů z praxe

VERLAG
DASHÖFER

21/2019

Monitoring zaměstnanců z pohledu GDPR

Cílem následujících řádků je podívat se na sledování zaměstnanců prostřednictvím moderní technologie z pohledu legislativy a nastínit řešení některých specifických požadavků.

Moderní technologie umožňující okamžité sdílení informací a relativně snadné analytické zpracování dat jsou velkým lákadlem pro zaměstnavatele ve smyslu možnosti sledovat výkony svých zaměstnanců či monitorovat využívání svěřených prostředků. Jejich zavádění v infrastruktuře, softwaru nebo hardwaru (např. v mobilních zařízeních) na pracovišti umožňují nové způsoby systematického a potenciálně invazivního zpracování dat. Například používání online služeb anebo lokačních údajů z chytrého zařízení jsou pro zaměstnance mnohem méně viditelné než tradičnější způsoby (např. neskryté kamery). Rovněž hranice mezi domovem a pracovištěm není úplně jasná – zaměstnanci mohou například pracovat z domova nebo během služební cesty.¹

PŘÁVNÍ RÁMEC

Primárním konfliktem, který musí současná i budoucí legislativa v této oblasti řešit, je **existence ochrany soukromí a ochrany osobních údajů** na jedné straně a zároveň **vlastnické právo zaměstnavatele** na straně druhé. Úkolem zákonodárců pak je vyřešit kolizi těchto dvou ústavně zaručených práv. Kromě toho zde existují ještě práva a povinnosti týkající se daného pracovního poměru. Podle ustanovení § 316 odst. 1 ZP **nesmí zaměstnanec využít pro svou osobní potřebu jakýkoliv výrobní či pracovní prostředek zaměstnavatele**, aniž by k takovému užití měl jeho souhlas. Dle judikatury je rozsah souhlasu pro použití pracovních a vý-

robních prostředků k osobní potřebě zcela na vůli zaměstnavatele. Zákaz použití se týká i **výpočetní techniky a telekomunikačních prostředků** zaměstnavatele a je **absolutní**. Zaměstnanec je naopak povinen tyto výrobní prostředky používat pouze za účelem výkonu uložené práce a má povinnost řádného hospodaření s nimi.

Dne 25. 5. 2018 nabylo účinnosti Nařízení 2016/679 Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (tzv. GDPR), které vnáší do oblasti ochrany dat nový rozměr, a hlavně po-



Vážení a milí čtenáři,

moderní technologie skýtají řadu možností a jen těžko si bez nich umíme představit každodenní život, i když na ně občas zehráme. Často nás ale také svádějí k neplechám a ani zaměstnavatelé nejsou vůči tomu imunní. Je těžké odolat pokušení sledovat výkony svých zaměstnanců či monitorovat, jak využívají, případně zneužívají prostředky jim svěřené.

Dnešní vydání Zpravodaje proto věnujeme otázkám monitoringu zaměstnanců, na které se podíváme jak z pohledu GDPR, tak z pohledu rozhodnutí Nejvyššího soudu a Evropského soudu pro lidská práva. JUDr. Magda Janotová se ve svém obsáhlém příspěvku zaměří jak na kamerové systémy na pracovišti, tak na monitoring vozidel pomocí GPS technologie, sledování elektronické pošty či mobilního telefonu.

Přeji Vám pěkné dny.

Magda Janotová

OBSAH

Monitoring zaměstnanců z pohledu GDPR	1
O převelikém úkolu	8
Přehled judikatury trochu jinak ..	8

¹ Pracovní skupina WP29. Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti. Pracovní překlad. [online]. 2017 [cit. 15. 8. 2019] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30203



siluje její společenský význam. Jeho významným aspektem je **univerzální platnost pro všechny země EU**. V návaznosti na to pak v ČR nabyl účinnosti dne 24. 4. 2019 zákon č. 110/2019 Sb., o zpracování osobních údajů, upřesňující GDPR (tzv. „adaptační zákon“) *Pozn.: Dřívější národní zákony (v ČR zákon č. 101/2000 Sb., o ochraně osobních údajů) bohužel vycházely ze značně zastaralé evropské směrnice (Směrnice 95/46/ES Evropského parlamentu a Rady ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů), v současné době jsou již neúčinné, proto nejsou v dalším textu analyzovány.*

GDPR A ZÁKONNOST ZPRACOVÁNÍ

Do oblasti monitoringu zaměstnanců zavádí GDPR celou řadu nových pravidel, která vycházejí ze zásad tohoto Obecného nařízení (čl. 5 GDPR). Zaměstnavatel je proto povinen zavedení monitorovacího systému a jeho nezbytnost nejen řádně odůvodnit ve smyslu legitimity těchto prostředků, ale také právně posoudit, zda jsou pro zavedení monitorovacích prostředků splněny veškeré podmínky vyžadované právním řádem. Ještě před zahájením zpracování by měl být proveden tzv. **test proporcionality**, aby se posoudilo, zda je dané zpracování k naplnění oprávněného účelu nutné, a aby se zvažila opatření nezbytná pro zajištění, že pravděpodobnost porušení práva na soukromý život a důvěrnost komunikací bude snížena na minimum.

Pro většinu zpracování dat na pracovišti **nemůže a neměl by být** právním důvodem souhlas zaměstnance (článek 7, písm. a) vzhledem k povaze vztahu mezi zaměstnavatelem a zaměstnancem. Zpracování osobních údajů nemůže být legalizováno zaměstnaneckým souhlasem tam, kde nesouhlas by vedl ke skutečné nebo možné újmě, což v souvislosti se zaměstnáním může být vysoce pravděpodobné, hlavně týká-li se to průběžného sledování zaměstnance zaměstnavatelem. Souhlas by pak nemohl být v žádném případě svobodný, jelikož se musí jednat o konkrétní a informovaný projev zaměstnancovy vůle. Vzhledem k nerovnováze sil mohou zaměstnanci udělit svobodný souhlas jen za výjimečných okolností, kdy souhlas nebo odmítnutí nevyvolá žádné následky².

Velmi častým legitimním důvodem pro zpracování osobních údajů při monitoringu je **oprávněný zájem**. Ten může spočívat v ochraně majetku anebo prokazování důležitých skutečností či vyplývat z důvodu

bezpečnosti práce. Účel zpracování však musí být oprávněný a zvolená metoda nebo konkrétní technologie zpracování musí být nezbytná pro naplnění oprávněného zájmu zaměstnavatele. Zpracování také musí být proporcionální vzhledem k podnikatelským potřebám, tj. odpovídat danému účelu. Zpracování dat na pracovišti by mělo být prováděno co možná nejméně vtravým způsobem a být zaměřeno na specifickou rizikovou oblast. Test proporcionality (pro splnění zásady proporcionality a subsidiarity) by měl být proveden před nasazením jakéhokoliv monitorovacího nástroje, aby se zvažilo, zda jsou všechna data potřebná, zda dané zpracování nepřevažuje nad obecnými právy ohledně soukromí, kterých zaměstnanci požívají i na pracovišti, a jaká opatření je třeba učinit pro zajištění, že zásahy do práva na soukromý život a práva na důvěrnost komunikace budou omezeny na nezbytné minimum.

S oprávněným zájmem souvisí také **právo zaměstnance na námitku vůči zpracování ze závažných a legitimních důvodů**. GDPR posiluje systém práv subjektů údajů, a to jak v aktualizaci stávajících práv, tak i některými novými právy, jako je např. právo na přenositelnost. Jejich účelem je vybalancovat vztah mezi správcem a subjektem údajů.

Operace zpracování musí také být ve shodě s **požadavky transparentnosti** (články 10 a 11 GDPR) a zaměstnanci by měli být jasně a plně informováni o zpracování svých údajů, včetně přítomnosti jakéhokoliv sledování. Měli by být informováni rovněž i rozsahu kontroly a o způsobu jejího provádění – kde a po jakou dobu budou údaje uchovávány, kdo k nim má přístup, kdo bude kontrolu provádět a jakým způsobem. Dále je nutno uvést informace o době a způsobu uložení shromážděných informací a informace o provedených technicko-organizačních opatřeních mimo jiné z důvodu minimalizace rizika jejich úniku.

GDPR A MONITOROVÁNÍ

Jak je naznačeno v dalším textu, dopouští se zaměstnavatelé často různých pochybení. Např. o způsobu kontroly a důvodech monitoringu rozhodoval i v minulosti ELSP v rozhodnutí ze dne 12. ledna 2016 č. 61496/08, Bărbulescu proti Rumunsku. V tomto procesu byl stěžovatel zaměstnán v soukromé společnosti jako inženýr v oddělení prodeje. Na žádost zaměstnavatele si založil účet na Yahoo Messenger, aby mohl odpovídat na žádosti zákazníků. V červenci 2007 jej zaměstnavatel informoval o tom, že jeho komunikace na tomto účtu byla v předchozích osmi dnech monitorována a že ze záznamů vyplývá, že jej v rozporu s vnitřními pravidly společnosti vyžival rovněž k soukromým účelům. Stěžovatel to popřel, poté mu však bylo předloženo jako důkaz 45 stran přepisu jeho komunikace včetně komunikace s jeho bratrem a snoubenkou. Společnost stěžovatele následně propustila pro porušení vnitřních předpisů, které kromě jiného zakazují používat počítače a další elektronická zařízení společnosti k soukromým účelům. Stěžovatel se bránil proti ukončení pracovního poměru u soudu, kde poukazoval na porušení svého soukromí a korespondence.³

Porušení shledal ESLP zejména v tom, že zaměstnavatel předem neinformoval zaměstnance o možnosti a rozsahu sledování jeho soukromé korespondence na Yahoo Messengeru. Podstatné však je, že ESLP potvrdil, že **zaměstnavatel má právo na monitorování komunikace zaměstnanců, pokud k tomu má legitimní důvod**. Tímto legitimním

² Škorníčková, Eva. Důvěřuj, ale prověřuj? GDPR zpřísňuje monitoring zaměstnanců [online]. 2018 [cit. 15.8.2019] Dostupné z <https://www.gdpr.cz/blog/monitoring-zamestnancu>

³ Murad, M. Uhrinová, A. Monitoring činnosti zaměstnanců ze strany zaměstnavatele [online]. 2019 [cit. 15.8.2019]. Dostupné z <https://www.epravo.cz/top/clanky/monitoring-cinnosti-zamestnancu-ze-strany-zamestnavatele-1-cast-109563.html>

důvodem může být (jako v tomto případě) podezření ze zneužívání pracovních nástrojů k soukromým účelům nebo například kontrola kvality péče o klienty či nutnost přístupu do e-mailové schránky zaměstnance v době jeho dovolené (za předpokladu, že toto nelze zařídit jinak). V úvahu je nutné také vzít, zdali je sledován tok komunikace, nebo i její obsah, zdali byla sledována celá komunikace, nebo pouze její část, či zda byl např. omezen počet osob, který měl ke sledované komunikaci přístup. Jinými slovy, zda je míra zásahu do soukromí **relevantní a přiměřená**. Základním předpokladem pro uvažování o zavedení sledování komunikace však v intencích rozhodnutí ESLP je povinnost zaměstnavatele o těchto nástrojích zaměstnance transparentně informovat.

V obdobném případě kontroly zaměstnanců rozhodoval také v minulosti Nejvyšší soud ve svém rozhodnutí ze dne 16. srpna 2012, sp. zn. 21 Cdo 1771/2011. V tomto případě zaměstnanec v září 2009 v rámci pracovní doby **strávil přes 102 hodin prohlížením internetových stránek, které neměly spojitost s plněním jeho pracovních úkolů**. Od prohlížení internetových stránek zaměstnanec neodradil ani zákaz v pracovním řádu zaměstnavatele. Zaměstnavatel na základě provedené kontroly uvedené porušení povinností zjistil a se zaměstnancem **okamžitě zrušil pracovní poměr pro zvlášť hrubé porušení pracovních povinností**. Zaměstnanec tvrdil, že prohlížení internetových stránek nebylo na úkor plnění jeho pracovních povinností. Dále připustil, že zřejmě porušil nějakou povinnost, ale že se nejednalo o porušení povinností zvlášť hrubým způsobem. To ostatně i potvrdil i NS – zaměstnanec porušil svoje pracovní povinnosti dle ustanovení § 38 odst. 1 písm. b) ZP a § 316 odst. 1 ZP a pracovního řádu zaměstnavatele tím, že porušil **výslovný zákaz bez souhlasu zaměstnavatele užívat pro svou osobní potřebu jeho výrobní a pracovní prostředky** včetně výpočetní techniky a povinnost zaměstnance plně **využívat pracovní dobu k plnění pracovních úkolů**. K námitce zaměstnance, že zaměstnavatel tajně sledoval jeho užívání internetu, NS připustil, že **kontrola dodržování** výše uvedených povinností nemůže být vykonávána zcela libovolně, ale **musí být prováděna přiměřeným způsobem**. Přiměřenost kontroly je nutné zkoumat vždy **s přihlédnutím k rozhodujícím okolnostem každého konkrétního případu**. Zejména je nutné vzít v úvahu, zda šlo o kontrolu průběžnou či následnou a jaká byla délka a rozsah kontroly. Podstatné také je to, zda a do jaké míry kontrola omezovala zaměstnance v jeho činnosti a do jaké míry zasahovala do jeho práva na soukromí. V tomto případě však smyslem provedené kontroly bylo zjištění, zda zaměstnanec respektuje zákaz užívat pro svou osobní potřebu výpočetní techniku zaměstnavatele vyplývající ze zákoníku práce a zda respektuje zákaz prohlížení internetových stránek, které s výkonem práce nesouvisí, vyplývající z vnitřního předpisu zaměstnavatele. Nebylo tedy kontrolováno, které internetové stránky zaměstnanec sleduje, a proto kontrola směřovala jen k ochraně majetku zaměstnavatele.

Z výše uvedeného tedy vyplývá, že je důležité **stanovit ve vnitřním předpisu pravidla týkající se využívání zařízení zaměstnavatele pro soukromé účely a kritéria pro provádění kontroly dodržování těchto pravidel**. Zejména je vhodné stanovit, kdo a v jakém rozsahu je oprávněn u zaměstnavatele kontrolu provést s tím, že větší důraz by měl být kladen na kontrolu následnou (kdy už existuje nějaké podezření). Vždy je však ale nutno **posuzovat každý případ zvlášť**, a to rovněž s ohledem na legitimní očekávání soukromí zaměstnanců, a ve svém výsledku poskytovat zaměstnancům neomezenou minimální úroveň soukromí, která se vždy uplatní. Také je potřeba dbát na to, aby osobní

údaje z monitorovacích zařízení byly přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány. Je nezbytné zejména zajistit, aby byla doba, po kterou jsou osobní údaje uchovávány, omezena na nezbytné minimum.

Zaměstnavatel jako správce osobních údajů je odpovědný za jakékoliv zpracování osobních údajů jím prováděné nebo prováděné pro něj. Zaměstnavatel je zejména povinen zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování jsou v souladu s GDPR, včetně účinnosti opatření. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob. Před zahájením monitorování by měl zaměstnavatel provést důkladnou analýzu toho, jaké zájmy monitorováním zaměstnanců chránit, a zvážit, zda nelze zájmy či majetek chránit jiným způsobem než monitorováním zaměstnanců. Pokud určitý druh zpracování, zejména při využití nových technologií a s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, ukládá GDPR v článku 35 pro tyto případy novou povinnost správcům zpracovat posouzení vlivu na ochranu osobních údajů (tzv. „posouzení vlivu“). Příkladem může být docházkový systém za využití biometrických údajů (fotografie zorničky nebo otisk prstu), který je novou technologií aplikovanou na zaměstnance. Pokud z posouzení vlivu vyplýne, že zjištěné riziko správce sám nezvládne ošetřit (zbytkové riziko zůstává vysoké), musí se pak obrátit na dozorový úřad a **konzultovat takovou situaci ještě před zahájením zpracování**.⁴

Velmi specifická situace nastává v případě, kdy jsou osobní údaje **zaměstnanců předávány mimo EU/EHP** (např. prostřednictvím cloudových služeb). V takovém případě je dle GDPR nutno zajistit, aby přístup jinými subjekty k zaměstnaneckým osobním údajům v rámci skupiny zůstal omezen na nezbytné minimum pro naplnění zamýšlených účelů. Kromě toho **musí** pro takovou zemi existovat rozhodnutí Komise, které určuje, zda je v ní zajištěna odpovídající úroveň ochrany. Pokud rozhodnutí Komise v této zemi neexistuje, mohou být osobní údaje do třetí země předány, pouze pokud přijímající správce poskytne vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektu údajů. Mezi tyto vhodné záruky patří zejména závazná podniková pravidla a standardní smluvní doložky. Vyjma shora uvedených podmínek lze předávání osobních údajů uskutečnit, pokud je splněna alespoň jedna z podmínek uvedených v článku 49 odst. 1 GDPR, např. v případě informovaného výslovného souhlasu subjektu údajů, nebo pokud je takové předání nezbytné pro splnění smlouvy mezi subjektem údajů a správcem osobních údajů.

V návaznosti na shora uvedené povinnosti zde však nastávají další otázky, a to ohledně přípustnosti využití monitorovacích systémů na pracovišti. Moderní technologie totiž umožňují v průběhu času sledovat zaměstnance na pracovišti i doma pomocí mnoha různých zařízení, jako jsou chytré telefony, osobní počítače, tablety, vozidla a nositelná elektronika. Není-li zpracování omezeno a transparentní, hrozí velké riziko, že zákonný zájem zaměstnavatele zvýšit efektivitu a chránit firemní majetek se promění v neodůvodnitelné a dotěrné sledování. V následující

⁴ Nešpůrek, P. Šuchman, J. Jaroš, J. Monitoring zaměstnanců: Práva a povinnosti zaměstnavatelů při zpracování osobních údajů [online]. 2019 [Cit. 15.8.2019]. Dostupné z <https://www.pravniprostor.cz/clanky/pracovni-pravo/monitoring-zamestnancu-prava-a-povinnosti-zamestnavatele-pri-zpracovani-osobnich-udaju>



části budou rozebrány jednotlivé případy monitoringu, které se v pracovních vztazích nejčastěji vyskytují.

KAMEROVÉ SYSTÉMY SE ZÁZNAMEM NA PRACOVISTI

Provozování kamerového systému se záznamem je považováno za zpracování osobních údajů podléhající povinností podle obecného nařízení, jelikož údaje uchovávané v záznamovém zařízení (obrazové či zvukové) jsou osobními údaji. To ovšem za předpokladu, že na základě těchto záznamů (informace z obrazových či zvukových nahrávek) lze přímo či nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud jsou ze snímku, na němž je zachycena, patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby.

Účelem provozu kamerového systému je ochrana života, zdraví a majetku zákazníků, ochrana života, zdraví a majetku zaměstnanců a ochrana majetku zaměstnavatele. Kamerové systémy však nejsou zárukou zamezení vzniku nežádoucí události, mají však významný vliv například na možnost následného uplatnění práv poškozených a zabránění opakování takové činnosti v budoucnu, jakož i představují odstrašující prvek, aby vůbec k protiprávnímu jednání nedocházelo. Kritérium potřebnosti vychází z nemožnosti uplatnit méně invazivní prostředky k dosažení cíle sledovaného správcem osobních údajů.

Zpracování osobních údajů provozováním kamerového systému je zákonné, pouze pokud je prováděno v odpovídajícím rozsahu v rámci některého z přípustných právních titulů zpracování osobních údajů, nejčastěji na pracovišti to bude zpracování nezbytné pro účely oprávněných zájmů příslušného zaměstnavatele (správce). Kamerové sledování **nesmí nadměrně zasahovat do soukromí**. Je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy) a rovněž nesmí docházet kromě minimalizovaného rozsahu ke sledování prostorů určených pro jejich „soukromé“ aktivity, jako jsou šatny a odpočinkové místnosti. Provoz kamer a využití záznamu musí být rovněž v souladu s pracovní právními předpisy, zejména § 316 ZP, zejména není přípustné sledování zaměstnanců v průběhu výkonu jejich práce. Ustanovení § 316 ZP umožňuje zaměstnavateli zaměstnance monitorovat a jinak narušovat jeho soukromí pouze ze závažných důvodů spočívajících ve zvláštní povaze činnosti zaměstnavatele.

V případě, že takový důvod dán není, nemůže se zaměstnavatel ke sledování uchýlit, a to ani za předpokladu, že zaměstnanec udělí s monitorováním souhlas. Tento závěr je založen na skutečnosti, že v případě § 316 odst. 2 ZP se jedná o kogentní právní normu, od níž není možné se odchýlit ani dohodou smluvních stran. Shromažďovat osobní údaje

lze pouze k stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Zpracovávat osobní údaje je možno pouze v souladu s účelem, k němuž byly shromážděny.

Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. V případě, pokud by docházelo vedle obrazového záznamu též k pořizování zvukového záznamu, je třeba posoudit, zda je jeho pořizování v souladu s účelem zpracování a je skutečně nezbytné nutné pro naplnění účelu zpracování. V drtivé většině případů tomu tak není (pro prokázání určité události zcela postačuje obrazový záznam). Rozsah zpracováváných údajů by se tedy měl omezit pouze na pořizování obrazového záznamu.

Povinností správce (zaměstnavatele) dle GDPR je v souvislosti s pořizováním kamerového záznamu vést záznamy o činnostech zpracování. Tato povinnost ovšem není úplně nová, záznamy fakticky nahrazují dosavadní registrační formuláře, na rozdíl od dosavadní registrace však tyto záznamy již správce pouze uchovává, tj., nezasílá Úřadu. Kromě již výše zmíněné informační povinnosti musí zaměstnavatel také přijmout veškeré potřebné technicko-organizační opatření pro zajištění ochrany zpracováváných osobních údajů a veškeré operace s kamerovým systémem logovat.

Pokud zaměstnavatel využívá v souvislosti s provozováním kamerového systému zpracovatele, je novou povinností **uzavřít s tímto zpracovatelem zpracovatelskou smlouvu** s obligatorními náležitostmi dle GDPR.

ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ ZAMĚSTNANCŮ PROSTŘEDNICTVÍM SOCIÁLNÍCH SÍTÍ

Prověřování zaměstnaneckých profilů na sociálních sítích by se nemělo dít na obecném základě. Není možné, aby zaměstnavatelé prověřovali zaměstnance nebo uchazeče o zaměstnání prostřednictvím sběru o jejich přátelích, volnočasových aktivitách, názorech, zájmech o jejich chování atd. Taktéž nemohou ani požadovat přístup k těmto informacím. Pokud však může zaměstnavatel doložit, že takové sledování je potřebné k ochraně jeho zákonných zájmů a že neexistují jiné, méně invazivní prostředky, přičemž bývalí zaměstnanci byli náležitě informováni o míře pravidelného sledování jejich veřejné komunikace, pak se zaměstnavatel může opírat o právní základ. Příkladem může být monitoring profilů bývalých zaměstnanců vázaných konkurenční doložkou na profesní sociální síti (LinkedIn).

ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S EVIDENCÍ PRACOVNÍ DOBY A DOCHÁZKY

Povinnost vést řádnou evidenci pracovní doby zaměstnanců vychází z § 96 ZP, přičemž není vyznačena žádná forma této evidence. Zaměstnavatel obvykle vede evidenci prostřednictvím speciálních docházkových systémů. Často se k identifikaci zaměstnanců využívají identifikační karty nebo elektronické čipy. Vyloučena není ani biometrická identifikace například prostřednictvím otisků prstů. V současné době využívají rovněž zaměstnavatelé i jiné systémy, které jim umožňují kontrolovat, kdo vstupuje, resp. může vstoupit, do jejich prostor anebo do jejich určitých částí, což může umožňovat také sledování činnosti zaměstnanců. Ačkoliv tyto systémy existují již řadu let, jsou nové technologie ke sledování pracovní doby a docházky využívány mnohem více, a to včetně takových, které

zpracovávají biometrická data, nebo prostředků ke sledování mobilních zařízení.

Stálé monitorování četnosti a času vstupu a odchodu zaměstnanců bude neodůvodnitelné, pokud budou takto získané údaje použity pro jiný účel než ten, který je pro zaměstnavatele oprávněný, například pro hodnocení výkonu zaměstnance. Pokud je zpracování pro zaměstnavatele nutné a nepřevažuje nad právem na soukromý život zaměstnanců, může být podle článku 7 písm. f) **v oprávněném zájmu zaměstnavatele, pokud byli zaměstnanci o operaci zpracování náležitě informováni.**

MONITORING POMOCÍ SLEDOVACÍCH SYSTÉMŮ NA BÁZI GPS

V poslední době stále více zaměstnavatelů sahá po zařízení umožňujícím monitoring pohybu jejich vozidel, zejména jde o pohyb vozidla a jeho aktuální polohu, dobu jízdy, trasu, kterou vozidlo jelo, spotřebu paliva a kontrolu rychlosti pomocí jednoduchého sledovacího systému na bázi GPS. Zaměstnavatel však nesleduje data jen o vozidle, ale rovněž o zaměstnanci, který vozidlo používá, včetně řidičova chování. Určité technologie také umožňují nepřetržité sledování vozidla i řidiče (např. zapisovač událostí).

Opět však platí stejná zásada – pokud zaměstnavatel používá např. systém GPS nebo jinou sledovací techniku v oprávněném zájmu, to znamená např. proto, aby si splnil svoji právní povinnost vést knihu jízd nebo prokázal soulad s dalšími právními povinnostmi, je toto zpracování možné. Nejprve je však nutné posoudit, zda je zpracování pro tyto účely nezbytné a zda zavedení těchto opatření bude v souladu se zásadami proporcionality a solidarity. Rovněž je zapotřebí určitých opatření ze strany zaměstnavatele. Např. pokud je vozidlo využíváno zaměstnancem i pro soukromé účely, bude vhodným opatřením nabídnutí „odstupní“ možnosti (opt-out) v případě, že jede zaměstnanec svoji soukromou cestu sloužící k ochraně jeho soukromých dat (systém se přepne do „soukromého“ režimu).⁵

Zaměstnavatel musí také jasně **informovat zaměstnance o instalaci sledovacího zařízení ve firemním vozidle**, které řídí, a o tom, že jejich pohyb během používání auta je zaznamenáván a že, podle uplatněné technologie, může být zaznamenáváno i jejich řidičské chování. Nejlepším řešením je umístit takovou informaci viditelně v zorném poli řidiče.

MALÁ ODBOČKA DO ČESKÉ POŠTY

V předchozím textu byl popsán případ, kdy jsou sledovací zařízení umístěna na služebních vozech v majetku zaměstnavatele. Z minulosti je však znám případ sledování pomocí GPS samotných osob (zaměstnanců) v období od března 2012 do února 2013, který nejprve řešil Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“), a protože se se závěrečným verdiktem zaměstnavatel nespokojil a podal správní žalobu, tak řešil tento případ Městský soud v Praze (rozhodnutí sp. zn. 6A 42/2013-48).

Nejprve ÚOOÚ posuzoval oprávněnost používání GPS monitorovacího zařízení, kterým vybavila poštovní doručovatele Česká pošta a které po dobu jejich směny zaznamenávalo údaje o poloze v rozsahu délky trasy, čas strávený na trase, samotná prošlá trasa a vyhodnocení, zda se doručovatel pohyboval pouze po svém okrsku. Tento program s názvem „Mo-

onitoring listovních zásilek“ měl sloužit ke kontrole a optimalizaci doručovacích okrsků, z hlediska vytiženosti okrsku, zajištění obslužnosti a kontrole přetěžování. Tento důvod, zkvalitnění služeb v souladu se zákonem o poštovních službách, považovala Česká pošta za dostatečný k tomu, aby mohla tímto způsobem určitě zaměstnance sledovat.

Tohoto názoru však nebyl ÚOOÚ, který konstatoval, že k dosažení předmětného účelu postačovalo sledování v horizontu dnů či týdnů (nikoliv jednoho roku) a že stačilo zaznamenávat pouze dvojice párující místo a čas doručení, a nikoliv celou trasu obchůzek. ÚOOÚ tedy vyhodnotil sledování za závažné, protože nebylo proporcionální, bylo nedůvodné, dlouhotrvající a byl dotčen příliš vysoký počet zaměstnanců (7770 zaměstnanců).

V následném soudním řízení pak Česká pošta argumentovala, že ÚOOÚ porušil povinnost zjistit při kontrole skutečný stav věci, protože údaje získané z provozu technologie GPS lokalizace se údajně nepropojovaly s databází zaměstnanců, a navíc byla aplikace přístupná pouze na základě utajených přístupových údajů pouze vybraným osobám z managementu České pošty. Ani tyto osoby pak nemohly najít konkrétního doručovatele/doručovatelku, ale pouze prohlédnout mapy a časy navštívených adresních bodů v jednotlivých okrscích. Identifikovat konkrétního zaměstnance se nedalo i díky tomu, že v jednom doručovacím okrsku se podle rozpisu práce střídalo více doručovatelů. Pokud by však přesto identifikace konkrétního zaměstnance možná byla, dle názoru České pošty za osobní údaj není nutné považovat informaci o pohybu zaměstnance, ale za informaci o výkonu sjednané práce. Tedy i kdyby bylo v tomto případě používání GPS technologie posouzeno jako zpracování osobních údajů, tak by Česká pošta nepochybně byla oprávněna zpracovávat veškeré osobní údaje svých zaměstnanců, jelikož je to nezbytné pro realizaci zákonných práv a plnění zákonných povinností zaměstnavatele.

Dalším ze zásadních argumentů České pošty bylo, že je poskytovatelem služby ve veřejném zájmu a také subjektem vázaným povinnostmi zajistit dodržování listovního a poštovního tajemství ve smyslu čl. 13 LZPS a § 16 zákona o poštovních službách, a proto disponuje důvody zvláštního zřetele hodnými, proč má právo jako zaměstnavatel zvýšeně monitorovat pohyb svých doručovatelů, přičemž způsob, kterým tak činila a jakým následně pracovala s nashromážděnými údaji, nepředstavoval nepřiměřený zásah do soukromí zaměstnance.

ÚOOÚ se při soudním jednání k uvedené argumentaci vyjádřil tak, že právo na soukromí přetrvává i v momentě, kdy zaměstnavatel kontroluje výkon práce svých zaměstnanců (kritéria týkající se kontroly zaměstnanců byla již podrobněji popsána v úvodu tohoto článku). Dále podotkl, že činnost poštovního doručovatele nelze považovat za „zvláštní povahu činnosti zaměstnavatele“ jen proto, že se jedná o činnost ve veřejném zájmu, která podléhá listovnímu tajemství.

Městský soud v Praze pak posuzoval **tři kritéria** (vhodnost, potřebnost, proporcionalitu), která hodnotil ÚOOÚ. Ke kritériu potřebnosti (zdali opatření omezující základní právo umožňuje dosáhnout sledovaný cíl) se vyjádřil, že použitá technologie zaznamenávající celou trasu nemohla eliminovat případné lidské selhání doručovatele, které mohlo mít za následek porušení právních povinností žalobce podle poštovního zákona. Ke kritériu potřebnosti (porovnání zvoleného prostředku k ochraně práv, v tomto případě povinností stanovených žalobci v po-

⁵ Škorníčková, Eva. Důvěřuj, ale prověřuj? GDPR přišlňuje monitoring zaměstnanců [online]. 2018 [cit. 15.8.2019]. Dostupné z na <https://www.gdpr.cz/blog/monitoring-zamestnancu/>

tovními zákoně s jinými v úvahu připadajícími opatřeními, umožňujícími dosáhnout stejného cíle, avšak se zásahem do soukromí zaměstnanců v menší míře) konstatoval, že je sice možné, aby Česká pošta zpracovávala údaje o tom, která doručovací místa doručovatel navštívil, příp. čas jejich obslužení, nelze však sledovat zaměstnance po celou jeho pracovní dobu – tj., permanentně monitorovat a uchovávat data o celé jeho trase. S posledním kritériem, proporionalitou (porovnání obou v kolizi stojících práv – práva na soukromí zaměstnance a povinností žalobce zabezpečit kvalitu jím poskytovaných služeb v souladu s poštovním zákonem) soud souhlasil s vyjádřením ÚOOÚ, že v případě posuzovaného zpracování osobních údajů se jedná o nepřiměřený zásah do soukromí, jelikož doručovatelé nemají při výkonu své práce jakékoli soukromí, neboť je monitorován každý jejich pohyb a zaměstnanci jsou tak pod neustálým dozorem.⁶

Městský soud se tak zcela ztotožnil s dřívějšími závěry Úřadu v tom, že GPS monitoring poštovních doručovatelů se bohužel dotýká práv na ochranu soukromí těchto zaměstnanců a je tedy nepřiměřený. V rozhodnutí pak uvedl, že je třeba rozlišovat získávání informací zaměstnavatelem o výkonu práce zaměstnanci a shromažďování osobních údajů zaměstnanců. Kontrola výkonu práce prováděná zaměstnavatelem je oprávněná tehdy, jestliže nenarušuje soukromí zaměstnance na pracovišti s výjimkou závažných důvodů spočívajících ve zvláštní povaze činnosti zaměstnavatele.

ELEKTRONICKÁ POŠTA

Na elektronickou komunikaci činěnou z obchodních prostor se mohou vztahovat pojmy „soukromý život“ a „korespondence“ ve smyslu článku 8 odst. 1 Evropské úmluvy. K pojmu soukromí se vyjádřil i ESLP v **rozhodnutí ve věci Niemietz v. Německo** ze dne 16. 12. 1992, stížnost č. 13710/88, který konstatoval, že: „*respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.*“ V rámci svých pracovních aktivit má totiž většina lidí největší příležitost navazovat a rozvíjet vztahy s vnějším okolím, a proto právo na respektování soukromého života zahrnuje i právo na respektování soukromí v zaměstnání, neboť z tohoto rozhodnutí vyplývá, že v rámci pracoviště existuje ve vztahu k zaměstnanci značná míra soukromí, se kterou je nutné počítat a kterou je třeba chránit.

Rovněž podle GDPR smí zaměstnavatelé shromažďovat osobní údaje pro zákonné účely a zpracovávat je za náležitých podmínek (např. proporcionalita a nezbytnost, skutečný a přítomný zájem, zákonný, srozumitelný a transparentní způsob) a musí mít zákonný důvod ke zpracování osobních údajů shromážděných nebo vytvořených prostřednictvím elektronických komunikací.⁷

Skutečnost, že zaměstnavatel je vlastníkem elektronických prostředků, neznamená, že zaměstnanci nemají právo na důvěrnost své komunikace, ať už jde o údaje o poloze nebo korespondenci. Dle vyjádření ÚOOÚ je v tomto případě **podstatné, o jakou e-mailovou adresu se jedná** (o tzv. formát adresy). To má pak význam při určení, zda se vůbec jedná o zpracování osobních údajů (definice osobního údaje je obsa-

žena v GDPR). Není zde rozhodující, zda e-mailová adresa patří zaměstnavateli, ale pokud je složena ze jména a příjmení zaměstnance (např. Jan.Svoboda@doména.cz), tak takováto e-mailová adresa je sama o sobě vždy osobním údajem. Naproti tomu, věcně konstruovaná e-mailová adresa (např. info@doména.cz) je úřední elektronickou adresou.

Dle stanoviska ÚOOÚ zaměstnavatel **není oprávněn sledovat, monitorovat a zpracovávat obsah korespondence svých zaměstnanců**. Zaměstnavatel případně smí u svých zaměstnanců pouze sledovat počet došlých a odeslaných e-mailů, případně (tj., zejména vznikne-li podezření ze zneužití pracovních prostředků, resp. využití k jiným než pracovním účelům) včetně hlavičky, tj., komu píše a od koho je dostávají. Tato činnost je zpracováním osobních údajů zaměstnance, byť za uvedených podmínek oprávněným zpracováním, a je tedy nezbytné dodržovat všechny zákonem o ochraně osobních údajů stanovené povinnosti.⁸

Soukromý e-mail zaměstnance smí zaměstnavatel otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail, tj., lze-li tento závěr učinit na základě údajů uvedených v hlavičce a jestliže je pravděpodobné, že z objektivních důvodů, jako je dlouhodobá nemoc zaměstnance, by k jejímu vyřízení zaměstnancem mohlo dojít natolik pozdě, že by zaměstnavatel mohl utrpět újmu na svých právech. Zaměstnavatel tak fakticky využívá svého práva chránit majetek podle zákoníku práce. Při nařizování dovolené by měl zaměstnavatel předem přijmout taková opatření k zastupování, aby k poškození soukromí zaměstnance nedošlo.

Typická situace nastala např. na jedné vysoké škole, kdy po jmenování nového rektora mu byla znepřístupněna e-mailová schránka, kterou měl pod svým jménem na škole zřízenou, a naopak, byla zpřístupněna novému vedení školy. ÚOOÚ po zahájení kontroly zjistil, že ještě po devíti měsících stále adresa existuje a do došlé pošty má přístup nový rektor s odůvodněním, že se nejednalo o soukromou adresu, ale o adresu rektora školy, tudíž bylo třeba v případě např. urgency ověřit, zda do schránky bývalého rektora nedošla důležitá pošta určená vysoké škole, a ne osobě bývalého rektora. Vzhledem k tomu, že bývalý rektor nepoužíval dvě různé e-mailové schránky, z nichž jedna by se týkala pouze korespondence s ním jakožto s rektorem vysoké školy a druhá by obsahovala korespondenci s jeho osobou jakožto s učitelem nebo kolegou, je třeba považovat veškerou korespondenci v e-mailové schránce za jeho osobní, k níž má mít přístup pouze on, přestože k tomu je používán server školy. To, že jde o osobní schránku, je také zřejmé z toho, že ke své e-mailové poště má přístup pouze zaměstnanec po přihlášení svým jménem a heslem. Proto ve chvíli, kdy bývalý rektor přestal být rektorem a v daném případě i zaměstnancem školy, měla být jeho e-mailová schránka zrušena. Neexistuje žádný důvod, aby tato schránka ještě po devíti měsících existovala, a přitom k ní neměl bývalý rektor přístup. Pokud e-mailová schránka neexistuje, protože v instituci již nepůsobí osoba, která je adresátem, tato informace by měla být automaticky odesílateli sdělena a ten musí činit další kroky adekvátní tomuto poznatku. Problém, který škola viděla v nebezpečí z prodlení v případě korespondence adresované bývalému rektorovi, bylo třeba řešit jiným způsobem – kupříkladu zrušením osobní e-mailové schránky, automatickou infor-

⁶ Staňková, L. GDPR snadno a přehledně. Mladá fronta, ISBN 978-80-204-5108-8. Praha, 2018

⁷ Úřad pro ochranu osobních údajů. Stanovisko č. 2/2009 [online]. 2009 [cit. 10.8.2019]. Dostupné z https://www.uoou.cz/files/stanovisko_2009_2.pdf

⁸ Beneš, O. Za jakých podmínek je možné kontrolovat e-maily zaměstnance? [online]. 2018 [cit. 6.8.2019]. Dostupné z <https://www.epravo.cz/top/clanky/za-jakych-podminek-je-mozne-kontrolovat-e-maily-zamestnance-107090.html>

mativní odpovědi, žádosti o zaslání na adresu nového rektora. V žádném případě nebyla škola oprávněna prohlížet soukromou poštu svého bývalého zaměstnance.⁹

S ohledem na výše uvedené bude zákonné, pokud bude zaměstnavatel provádět tzv. **anonymní monitorování e-mailů**, které neumožňuje vyvodit závěry o konkrétních zaměstnancích a které neumožňuje tyto jednotlivce identifikovat. K tomu mohou zaměstnavatelům sloužit různé nástroje, které automaticky monitorují např. odchozí e-maily, za účelem ochrany osobních údajů, nebo může zaměstnavatel například provést namátkovou kontrolu hlaviček e-mailů. Pokud v případě např. běžné anonymní prohlídky budou zjištěny nesrovnalosti a bude existovat důvodné podezření, že zaměstnanec např. prozrazuje obchodní tajemství či páchá trestný čin, je možné provést cílené, adresné monitorování e-mailové komunikace. Zároveň má ale zaměstnavatel povinnost o možnosti provedení takového monitoringu zaměstnance předem informovat. Kontrolu e-mailů lze provést také v případě, že slouží k ochraně zaměstnanců při odhalování šikany či sexuálního obtěžování.

Stejná logika se podle odborníků aplikuje také při posuzování této problematiky skrze evropskou legislativu o ochraně osobních údajů (v současné době dle GDPR). V takovém případě je třeba mít na paměti, že takovéto zpracování může probíhat, pouze pokud zájmy zaměstnavatele nejsou převáženy základními právy subjektu údajů – zaměstnance, které jsou hodny ochrany.

TELEFON A SPRÁVA MOBILNÍCH ZAŘÍZENÍ

Ohledně sledování telefonních hovorů zaměstnavatelem se v minulosti vyjádřil i Evropský soud pro lidská práva, když v rozsudku ELSP ve věci **Coplandová v. Spojené království** ze dne 3. dubna 2007, stížnost č. 62617/00, v §§ 41 a 44 se vyslovil k otázce soukromí na pracovišti: „Na telefonní hovory z firemních prostor se podle předchozí judikatury soudy zcela jasně vztahují pojmy „soukromý život“ a „korespondence“ uvedené v čl. 8 odst. 1 (evropské Úmluvy o ochraně lidských práv a základních svobod, CETS 005, vyhlášené pod č. 209/1992 Sb.)“. Rovněž ve starším rozsudku ve věci **Halford proti Spojenému království** ze dne 25. 6. 1997 – odposlouchávání telefonních hovorů zaměstnavatelem, který chtěl prostřednictvím odposlechu zajistit důkazy pro účely jejich využití v pracovněprávním sporu, dovodil dle čl. 8 Úmluvy, že telefonní hovory uskutečněné z pracoviště i z domova „mohou spadat pod pojem soukromý život a korespondence“. Na možnost sledování telefonních hovorů nebyla zaměstnankyně upozorněna, a byla tedy oprávněna očekávat při těchto hovorech soukromí. Navíc jeden z telefonů měla výslovně určený na soukromou komunikaci za účelem řešení svého pracovněprávního sporu.¹⁰

Dalším možným úskalím může být **správa mobilních zařízení**, která zaměstnavatelům umožňuje zjistit polohu zařízení, provádět specifické konfigurace a/nebo instalovat aplikace či mazat „data-on-demand“. Tyto služby umožňují sledovat zařízení nebo z něj ukládat informace v reálném čase, dokonce i když není nahlášeno jako ukradené.

Toto zpracování však musí být v souladu se zásadou proporcionality a subsidiarity dle GDPR. Musí být tedy zajištěno, aby data získaná při zjišťování polohy na dálku byla zpracována pro stanovený účel a nebyla či nemohla být součástí rozsáhlejšího programu umožňujícího průběžné sledování zaměstnanců. I v případě, pokud budou data zpracována pro oprávněný účel, musí být zajištěno, aby sledovací funkce byly redukovány. Samozřejmě ještě před nasazením této technologie musí být zpracován test proporcionality, který ukáže, že tato technologie je pro zaměstnavatele nezbytná. Také zde nemůžeme zapomenout na informační povinnost, kdy zaměstnanci musí být informováni, jaké sledování probíhá a jaké důsledky pro ně může mít.

MONITORING V PŘÍPADĚ PRÁCE NA DÁLKU

V poslední době stále více přibývá případů, kdy zaměstnanci pracují z domova (práce z domova či práce na dálku). Zaměstnavatelé jim poskytují prostředky informační a komunikační techniky nebo software, který je nainstalován na jejich zařízení. Pro bezpečnost toku dat a vyloučení neoprávněného přístupu k těmto datům jsou zaměstnavatelem zavedena různá bezpečnostní opatření. Ti pak mají mylnou představu, že mohou pomocí těchto zařízení také monitorovat zaměstnancovu činnost či využití pracovní doby. Instalaci softwaru, který umí např. logovat úder kláves či pohyb myši, či instalaci webové kamery a následný sběr záznamů z této kamery berou v tomto případě jako odůvodnitelné. Takové technologie jsou také dnes na trhu pro zaměstnavatele lehce dostupnou záležitostí.

Výše uvedené zpracování osobních údajů je však **nepřiměřené** a těžko by k němu našli zaměstnavatelé právní důvod ke zpracování, protože je velmi nepravděpodobné, že ani oprávněný zájem správce pro toto zpracování by byl obhajitelný.

ZÁVĚR

Je zcela zřejmé, že i když po účinnosti GDPR musí firmy přemýšlet i nadále nad tím, zda nezasahují do soukromí zaměstnanců více, než je třeba, přibývá zaměstnavatelům více povinností. Zaměstnavatelé by měli v každém případě pamatovat na základní zásady zpracování osobních údajů (ať už je to zásada účelového omezení, omezení rozsahu a doby zpracování aj.), na soulad zpracování se zásadou subsidiarity a proporcionality, zaměstnanci by měli být o probíhající zpracování účinným způsobem informováni. Monitoring bude v praktické rovině v určitých případech možný za dodržení výše popsaných povinností a opatření, oprávněným zájmem zaměstnavatele tak zůstane například zabezpečení dat nebo kontrola využívání firemních prostředků. Oprávněný zájem by se ale těžko hledal pro plošný monitoring klávesnice za účelem zjištění, co dotyčný píše nebo vytváří v aplikaci. Souhlas nebude ve většině případů právním důvodem pro zpracování dat, ledaže by zaměstnanci měli možnost odmítnout, aniž by to pro ně mělo neblahé důsledky.

Zaměstnavatelé i při dodržování povinností dle GDPR nemají i tak právní jistotu v tom, že využívané kontrolní a sledovací mechanismy nad míru nezasahují do soukromí zaměstnanců. Rovněž předem oznámená kontrola bude ve většině případů kontraproduktivní. Současná legislativa bohužel řeší monitoring zaměstnanců zcela nekonkrétně, zaměstnavatelé proto musí **sledovat budoucí judikaturu** v této oblasti.

JUDr. Magda Janotová

⁹ Úřad pro ochranu osobních údajů. Obsah e-mailové schránky [online]. 2013 [cit. 22.8.2019]. Dostupné z <https://www.uoou.cz/obsah-e-mailove-schranky/d-6268/p1=1020>

¹⁰ Soukromí v práci ve světle evropské judikatury, Právní rádce, str. 36-41, Vydavatelství Economia, a.s., Ročník XXVII, číslo 7/8, ISSN 1210-4817