PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

17/CS

WP 249

Stanovisko 2/2017 ke zpracování údajů na pracovišti

Přijaté dne 8. června 2017

Obsah

1. Shrnutí

Toto stanovisko doplňuje předchozí zveřejněné dokumenty pracovní skupiny zřízené podle článku 29 (dále jen „pracovní skupina WP29“), *stanovisko č. 8/2001 ke zpracování osobních údajů v souvislosti se zaměstnáním* (WP48)[1] a *pracovní dokument* z roku 2002 *o dohledu nad elektronickými komunikacemi na pracovišti* (WP55)[2]. Od zveřejnění těchto dokumentů byla zavedena řada nových technologií umožňujících systematičtější zpracování osobních údajů zaměstnanců na pracovišti, což může vytvářet významné výzvy týkající se ochrany soukromí a údajů.

Toto stanovisko nově posuzuje rovnováhu mezi oprávněnými zájmy zaměstnavatelů a přiměřenými očekáváními zaměstnanců týkajícími se soukromí, a to tím, že naznačuje rizika představovaná novými technologiemi a provádí posouzení přiměřenosti řady scénářů, v nichž by mohly být tyto nové technologie využity.

Ačkoliv se stanovisko zabývá především směrnicí o ochraně údajů, zaměřuje se také na dodatečné povinnosti uložené zaměstnavatelům obecným nařízením o ochraně osobních údajů. Stanovisko rovněž znovu potvrzuje postoj a závěry ze stanoviska č. 8/2001 a pracovního dokumentu WP55, a sice že při zpracování osobních údajů zaměstnanců:

- by zaměstnavatelé měli mít neustále na paměti základní zásady ochrany údajů, bez ohledu na použitou technologii,
- požívá obsah elektronických komunikací uskutečněných z obchodních prostor stejnou ochranu základních práv jako analogové komunikace,
- je vysoce nepravděpodobné, že by souhlas mohl být právním základem pro zpracování údajů na pracovišti, pokud zaměstnanci nemohou udělení tohoto souhlasu odmítnout, aniž by to pro ně mělo nepříznivé důsledky,
- lze v některých případech uplatnit plnění smlouvy a oprávněné zájmy, je-li zpracování zcela nezbytné pro oprávněný zájem a je v souladu se zásadami proporcionality a subsidiarity,
- by zaměstnanci měli obdržet účinné informace o monitorování, k němuž dochází, a
- by k jakémukoliv předání údajů o zaměstnancích do jiné země mělo dojít pouze tehdy, je-li zajištěna odpovídající úroveň ochrany.

2. Úvod

Rychlé zavádění nových informačních technologií na pracovišti, pokud jde o infrastrukturu, aplikace a inteligentní zařízení, umožňuje nové druhy systematického a potenciálně invazivního zpracování údajů na pracovišti. Zde jsou některé příklady:

[1] Pracovní skupina WP29, *stanovisko č. 8/2001 ke zpracování osobních údajů v souvislosti se zaměstnáním*, WP 48, 13. září 2001, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] Pracovní skupina WP29, *pracovní dokument o dohledu nad elektronickými komunikacemi na pracovišti*, WP 55, 29. května 2002, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- Technologie umožňující zpracování údajů na pracovišti nyní mohou být zaváděny za zlomek nákladů než před několika lety, přičemž kapacita pro zpracování osobních údajů těmito technologiemi se exponenciálně zvýšila.
- Nové formy zpracování, jako například zpracování osobních údajů o používání on-line služeb a/nebo lokalizačních údajů z inteligentních zařízení, jsou pro zaměstnance mnohem méně viditelné než jiné tradičnější druhy, jako například průmyslové kamery. To vyvolává otázky ohledně míry, do jaké jsou si zaměstnanci těchto technologií vědomi, jelikož zaměstnavatelé mohou tato zpracování zavádět nezákonně, aniž by to zaměstnancům předem oznámili.
- Hranice mezi domovem a pracovištěm jsou stále méně znatelné. Například pracují-li zaměstnanci vzdáleně (např. z domova) nebo jsou-li na služební cestě, může docházet k monitorování činností mimo fyzické pracovní prostředí, které může případně zahrnovat monitorování fyzické osoby v soukromém kontextu.

Používání těchto technologií sice může být užitečné při zjišťování ztrát v oblasti duševního vlastnictví a hmotného majetku společnosti nebo jejich předcházení, při zlepšování produktivity zaměstnanců a při ochraně osobních údajů, za které správce údajů odpovídá, ale tyto technologie rovněž vytvářejí významné výzvy týkající se ochrany soukromí a údajů. V důsledku toho je nutné provést nové posouzení rovnováhy mezi oprávněným zájmem zaměstnavatele chránit své podnikání a přiměřenými očekáváními ohledně soukromí subjektů údajů, tedy zaměstnanců.

Toto stanovisko se zaměřuje na nové informační technologie, a to prostřednictvím posouzení devíti různých scénářů, v nichž mohou být tyto technologie využity, avšak stručně se zabývá rovněž tradičnějšími metodami zpracování údajů na pracovišti, kde jsou zesílena rizika v důsledku technologických změn.

Kde se v tomto stanovisku používá slovo „zaměstnanec“, pracovní skupina WP29 nemá v úmyslu omezit rozsah tohoto pojmu pouze na osoby s pracovní smlouvou uznávanou podle platných pracovněprávních předpisů. Během posledních desetiletí začaly být mnohem běžnější nové obchodní modely, které jsou zajišťovány různými druhy pracovních vztahů, a zejména samostatná výdělečná činnost. Toto stanovisko je určeno k pokrytí veškerých situací zahrnujících pracovní poměr, bez ohledu na to, zda je tento poměr založen na pracovní smlouvě.

Je důležité uvést, že zaměstnanci jsou vzhledem k závislosti vyplývající ze vztahu zaměstnavatel/zaměstnanec zřídkakdy schopni svobodně udělit, odmítnout nebo zrušit souhlas. Pokud se nebude jednat o výjimečné situace, budou se zaměstnavatelé muset spoléhat na jiný právní základ než souhlas – jako například na nutnost zpracovat údaje pro svůj oprávněný zájem. Oprávněný zájem však sám o sobě není dostatečný pro to, aby převážil nad právy a svobodami zaměstnanců.

Bez ohledu na právní základ pro takové zpracování by měl být před zahájením zpracování proveden test přiměřenosti, aby se zvážilo, zda je zpracování nezbytné pro dosažení oprávněného zájmu, a aby se zvážila také opatření, která je nutné přijmout za účelem zajištění toho, že případy porušení práva na soukromý život a práva na důvěrnost komunikací jsou omezeny na minimum. Toto může tvořit součást posouzení vlivu na ochranu osobních údajů.

3. Právní rámec

Ačkoliv níže uvedená analýza byla provedena především v souvislosti se stávajícím právním rámcem podle směrnice 95/46/ES (dále jen „směrnice o ochraně údajů“)[3], toto stanovisko se zaměřuje také na povinnosti podle nařízení 2016/679 (dále jen „obecné nařízení o ochraně osobních údajů“)[4], které již vstoupilo v platnost a nabyde účinnosti dne 25. května 2018.

Pracovní skupina s ohledem na navrhované nařízení o soukromí a elektronických komunikacích[5] vyzývá evropské zákonodárce, aby vytvořili zvláštní výjimku pro zásahy do zařízení vydaných zaměstnancům[6]. Navrhované nařízení totiž neobsahuje vhodnou výjimku z obecného zákazu zasahování a zaměstnavatelé obvykle nemohou poskytnout platný souhlas se zpracováním osobních údajů svých zaměstnanců.

3.1 Směrnice 95/46/ES – směrnice o ochraně údajů

Pracovní skupina WP29 ve svém stanovisku č. 8/2001 již nastínila, že zaměstnavatelé při zpracování osobních údajů v souvislosti se zaměstnáním zohledňují základní zásady ochrany údajů stanovené směrnicí o ochraně údajů. Vývoj nových technologií a nové metody zpracování v této souvislosti situaci nezměnily – lze ale konstatovat, že tento vývoj *zvýšil důležitost* toho, aby tak zaměstnavatelé činili. Zaměstnavatelé by tudíž měli:

- zajistit, že údaje jsou zpracovávány pro stanovené a oprávněné účely, které jsou přiměřené a nezbytné,
- zohlednit zásadu omezení účelu a zároveň se ujistit, že údaje jsou přiměřené, podstatné a v množství úměrném oprávněnému účelu,
- uplatnit zásady proporcionality a subsidiarity, bez ohledu na použitelný právní základ,
- být transparentní vůči zaměstnancům, pokud jde o použití a účely monitorovacích technologií,
- umožnit výkon práv subjektu údajů, a to včetně práva na přístup a podle daného případu práva na opravu, výmaz nebo blokování osobních údajů,
- uchovávat přesné údaje a neuchovávat je po delší dobu, než je nezbytně nutné, a
- přijmout veškerá nezbytná opatření na ochranu údajů proti neoprávněnému přístupu a zajistit, že zaměstnanci si jsou dostatečně vědomi povinností týkajících se ochrany údajů.

Pracovní skupina WP29 nemíní opakovat své dřívější pokyny, ale ráda by zdůraznila tři zásady, konkrétně: právní základ, transparentnost a automaticky přijímaná rozhodnutí.

3.1.1 *PRÁVNÍ ZÁKLAD (ČLÁNEK 7)*

[3] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. L 281, 23.11.1995, s. 31–50, internetová stránka: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:31995L0046

[4] Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016 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), *Úř. věst. L 119, 4.5.12016, s. 1–88*, internetová stránka: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679

[5] Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES, 2017/0003 (COD), internetová stránka: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1508346397687&uri=CELEX:52017PC0010&from=CS

[6] Viz pracovní skupina WP29, *stanovisko č. 01/2017 k návrhu nařízení o soukromí a elektronických komunikacích*, WP 247, 4. dubna 2017, strana 29; internetová stránka: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

Při zpracování osobních údajů v souvislosti se zaměstnáním musí být splněno alespoň jedno z kritérií stanovených v článku 7. Pokud druhy zpracovávaných osobních údajů zahrnují zvláštní kategorie (jak je podrobně uvedeno v článku 8), je zpracování zakázáno, pokud se neuplatní výjimka[7,8]. I když zaměstnavatel může uplatnit jednu z těchto výjimek, aby bylo zpracování oprávněné, je stále vyžadován právní základ z článku 7.

Souhrnně lze říci, že zaměstnavatelé proto musí vzít na vědomí následující:

- pro většinu zpracování údajů na pracovišti **právním základem nemůže být, a ani by neměl být, souhlas zaměstnanců** (čl. 7 písm. a)), a to vzhledem k povaze vztahu mezi zaměstnavatelem a zaměstnancem,
- zpracování může být nezbytné pro **plnění smlouvy** (čl. 7 písm. b)) v případech, kdy zaměstnavatel musí osobní údaje zaměstnance zpracovat, aby každý takový závazek splnil,
- je poměrně běžné, že **pracovní právo může ukládat právní povinnosti** (čl. 7 písm. c)), **které vyžadují zpracování osobních údajů**; v takových případech musí být zaměstnanec o tomto zpracování jasně a plně informován (pokud se neuplatní výjimka),
- pokud se zaměstnavatel rozhodne opírat o **oprávněný zájem** (čl. 7 písm. f)), musí být účel zpracování oprávněný, zvolená metoda nebo konkrétní technologie musí být nezbytná, přiměřená a uplatněná co nejméně rušivým způsobem, a zároveň musí zaměstnavateli umožňovat prokázat, že **byla zavedena vhodná opatření** k zajištění rovnováhy se základními právy a svobodami zaměstnanců[9],
- operace zpracování musí rovněž splňovat **požadavky na transparentnost** (články 10 a 11) a zaměstnanci by měli být o zpracování svých osobních údajů jasně a plně informováni[10], a to včetně informací o existenci jakéhokoliv monitorování, a
- za účelem zajištění bezpečného zpracování by měla být přijata **vhodná technická a organizační opatření** (článek 17).

Nejdůležitější kritéria podle článku 7 jsou podrobně popsána níže.

- **Souhlas (čl. 7 písm. a))**

Souhlas je podle směrnice o ochraně údajů definován jako jakýkoliv svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování. Aby byl souhlas platný, musí být také odvolatelný.

Pracovní skupina WP29 ve svém stanovisku č. 8/2001 již nastínila, že pokud zaměstnavatel musí zpracovat osobní údaje svých zaměstnanců, je zavádějící vycházet z předpokladu, že

[7] Jak je uvedeno v části 8 stanoviska č. 8/2001; například čl. 8 odst. 2 písm. b) stanoví výjimku v případech, kdy je zpracování nezbytné pro dodržení povinností a zvláštních práv správce v oblasti pracovního práva, pokud je k tomu oprávněn vnitrostátními právními předpisy, které stanoví příslušná ochranná opatření.

[8] Je třeba uvést, že v některých zemích jsou zavedena zvláštní opatření, která musí zaměstnavatelé za účelem ochrany soukromého života zaměstnanců dodržovat. Jednou ze zemí, kde tato zvláštní opatření existují, je například Portugalsko a podobná opatření mohou být uplatňována také v některých jiných členských státech. Závěry v oddíle 5.6, jakož i příklady uvedené v oddílech 5.1 a 5.7.1 tohoto stanoviska proto z těchto důvodů v Portugalsku neplatí.

[9] Pracovní skupina WP29, *stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES,* WP 217, přijaté dne 9. dubna 2014, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

[10] Podle čl. 11 odst. 2 směrnice o ochraně údajů je správce osvobozen od povinnosti poskytnout subjektu údajů informace v případech, kdy je zaznamenávání nebo shromažďování údajů výslovně stanoveno zákonem.

zpracování může být legitimizováno prostřednictvím souhlasu zaměstnance. V případech, kde zaměstnavatel uvede, že vyžaduje souhlas, a kde existuje skutečná nebo případná závažná předpojatost plynoucí z toho, že zaměstnanec nesouhlasí (což může být v souvislosti se zaměstnáním vysoce pravděpodobné, zejména pokud se jedná o situaci, kdy zaměstnavatel sleduje chování zaměstnance v průběhu doby), pak souhlas není platný, jelikož není, a ani nemůže být, svobodně udělen. Proto pro většinu případů zpracování údajů zaměstnanců právním základem tohoto zpracování nemůže být, a ani by neměl být, souhlas zaměstnanců, a je tedy vyžadován jiný právní základ.

Kromě toho i v případech, kdy by bylo možné souhlas považovat za platný právní základ takového zpracování (tj. kdy lze nepochybně dojít k závěru, že souhlas je udělen svobodně), se musí jednat o výslovný a vědomý projev vůle zaměstnance. Výchozí nastavení zařízení a/nebo instalace softwaru usnadňující zpracování elektronických osobních údajů nelze považovat za souhlas udělený zaměstnanci, jelikož souhlas vyžaduje aktivní vyjádření vůle. Nečinnost (tj. neprovedení změny výchozího nastavení) nelze obecně považovat za výslovný souhlas povolující takové zpracování[11].

- **Plnění smlouvy (čl. 7 písm. b))**

Pracovní poměry jsou často založeny na pracovní smlouvě mezi zaměstnavatelem a zaměstnancem. Při plnění povinností podle takové smlouvy, jako například při vyplácení zaměstnance, je zaměstnavatel povinen zpracovat některé osobní údaje.

- **Právní povinnosti (čl. 7 písm. c))**

Je poměrně běžné, že pracovní právo ukládá zaměstnavateli právní povinnosti, které vyžadují zpracování osobních údajů (např. za účelem výpočtu daně a administrace platů). V takových případech tyto právní předpisy jasně představují právní základ pro zpracování údajů.

- **Oprávněný zájem (čl. 7 písm. f))**

Pokud se zaměstnavatel chce opírat o právní základ čl. 7 písm. f) směrnice o ochraně údajů, musí být účel zpracování oprávněný a zvolená metoda nebo konkrétní technologie, s níž má být zpracování provedeno, musí být nezbytná pro oprávněný zájem zaměstnavatele. Zpracování musí být rovněž přiměřené podnikatelským potřebám, tj. účelu, který má splnit. Zpracování údajů na pracovišti by mělo být provedeno co nejméně rušivým způsobem a mělo by být zaměřeno na specifickou oblast rizika. Navíc při použití čl. 7 písm. f) si zaměstnanec zachovává právo na námitku vůči zpracování z vážných a legitimních důvodů podle článku 14.

Aby bylo možné jako právní základ pro zpracování použít čl. 7 písm. f), je nezbytné, aby byla přítomna specifická zmírňující opatření k zajištění řádné rovnováhy mezi oprávněným zájmem zaměstnavatele a základními právy a svobodami zaměstnanců[12]. Tato opatření by v

[11] Viz také pracovní skupina WP29, *stanovisko č. 15/2011 k definici souhlasu*, WP187, 13. července 2011, internetová adresa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf, strana 24.

[12] Jako příklad rovnováhy, kterou je třeba nastolit, lze uvést věc *Köpke v. Německo*, [2010] ESLP 1725, (internetová adresa: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), v níž byl zaměstnanec propuštěn v důsledku tajného videokamerového monitorování provedeného zaměstnavatelem a soukromou detektivní agenturou. Ačkoliv soud v tomto případě dospěl k závěru, že vnitrostátní orgány nastolily spravedlivou rovnováhu mezi oprávněným zájmem zaměstnavatele (ochrana jeho vlastnických práv), právem zaměstnance na

závislosti na formě monitorování měla zahrnovat omezení monitorování, aby bylo zaručeno, že není porušeno soukromí zaměstnance. Tato omezení mohou být:

- místní (např. monitorování pouze na specifických místech; monitorování citlivých prostor jako náboženských míst a například hygienických zázemí a místností určených k trávení přestávek by mělo být zakázáno),
- orientovaná na údaje (např. by neměly být monitorovány osobní elektronické soubory a komunikace), a
- časová (např. namátkové monitorování namísto nepřetržitého).

3.1.2 *TRANSPARENTNOST (ČLÁNKY 10 A 11)*

Na zpracování údajů na pracovišti se vztahují požadavky na transparentnost uvedené v článcích 10 a 11, tzn. že zaměstnanci musí být informováni o existenci jakéhokoliv monitorování, o účelu, za jakým mají být osobní údaje zpracovány, a o jakýchkoliv dalších informacích nezbytných pro zajištění řádného zpracování.

S novými technologiemi se význam transparentnosti zvyšuje, jelikož tyto technologie umožňují tajně shromažďovat a dále zpracovávat případná obrovská množství osobních údajů.

3.1.3 *AUTOMATIZOVANÁ ROZHODNUTÍ (ČLÁNEK 15)*

Článek 15 směrnice o ochraně údajů subjektům údajů rovněž přiznává právo nestát se subjektem rozhodnutí přijatého výlučně na základě automatizovaného zpracování, pokud toto rozhodnutí zakládá právní účinky, nebo pokud se jich významně dotýká, a pokud je toto rozhodnutí přijato výlučně na základě automatizovaného zpracování údajů určeného k hodnocení určitých osobních rysů, například pracovního výkonu, ledaže by toto rozhodnutí bylo nezbytné pro zahájení plnění smlouvy, povoleno právním předpisem Unie nebo členského státu, nebo založeno na výslovném souhlasu subjektu údajů.

3.2 Nařízení 2016/679 – obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údaje zahrnuje požadavky uvedené ve směrnici o ochraně údajů a zpřísňuje je. Zavádí rovněž nové povinnosti pro všechny správce údajů včetně zaměstnavatelů.

3.2.1 *ZÁMĚRNÁ OCHRANA OSOBNÍCH ÚDAJŮ*

Článek 25 obecného nařízení o ochraně osobních údajů ukládá správcům údajů povinnost provádět záměrnou a standardní ochranu osobních údajů. Například pokud zaměstnavatel zaměstnancům vydává zařízení a jsou-li jeho součástí monitorovací technologie, měla by být zvolena řešení, která co nejvíce respektují soukromí. Rovněž je třeba zohlednit minimalizaci údajů.

3.2.2 *POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ*

Článek 35 obecného nařízení o ochraně osobních údajů popisuje požadavky na správce údajů, aby prováděli posouzení vlivu na ochranu osobních údajů v případech, kdy je

---

respektování soukromého života a veřejným zájmem při výkonu spravedlnosti, rovněž uvedl, že v důsledku technologického rozvoje by v budoucnu mohla být různým dotčeným zájmům dána odlišná váha.

pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům samotného zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob. Příkladem je systematické a rozsáhlé vyhodnocování osobních rysů fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na jehož základě jsou přijímána rozhodnutí, jež vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad.

Pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že zjištěná rizika nemohou být správcem dostatečně řešena – tj., že zbytková rizika zůstávají vysoká –, pak musí správce před zahájením zpracování konzultovat dozorový úřad (čl. 36 odst. 1), jak je objasněno v pokynech pracovní skupiny WP29 týkajících se posouzení vlivu na ochranu osobních údajů[13].

3.2.3 „*ZPRACOVÁNÍ V SOUVISLOSTI SE ZAMĚSTNÁNÍM*“

Článek 88 obecného nařízení o ochraně osobních údajů stanoví, že členské státy mohou právním předpisem nebo kolektivními smlouvami stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním. Tato pravidla mohou být stanovena zejména za účelem:

- náboru,
- plnění pracovní smlouvy (včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami),
- řízení, plánování a organizace práce,
- zajištění rovnosti a rozmanitosti na pracovišti,
- zajištění zdraví a bezpečnosti na pracovišti,
- ochrany majetku zaměstnavatele nebo majetku zákazníka,
- (individuálního) výkonu a požívání práv a výhod spojených se zaměstnáním a
- ukončení zaměstnaneckého poměru.

V souladu s čl. 88 odst. 2 by tato pravidla měla zahrnovat zvláštní a vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, především pokud jde o:

- transparentnost zpracování,
- předávání osobních údajů v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a
- systémy monitorování na pracovišti.

Pracovní skupina poskytuje v předkládaném stanovisku pokyny pro oprávněné použití nových technologií v řadě konkrétních situací a podrobně uvádí zvláštní a vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv zaměstnanců.

4. Rizika

[13] Pracovní skupina WP29, *Pokyny týkající se posouzení vlivu na ochranu údajů a určující, zda je pravděpodobné, že zpracování povede k „vysokému riziku“ pro účely nařízení 2016/679*, WP 248, 4. dubna 2017, internetová adresa: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, strana 18.

Moderní technologie umožňují sledovat zaměstnance v průběhu doby, na pracovišti i doma, a to prostřednictvím řady různých zařízení, jako jsou například chytré telefony, stolní počítače, tablety, vozidla nebo nositelná zařízení. Pokud neexistují žádná omezení zpracování a pokud zpracování není transparentní, existuje vysoké riziko, že se z oprávněného zájmu zaměstnavatelů na zlepšení účinnosti a ochraně aktiv společnosti stane neodůvodněné a rušivé monitorování.

Technologie monitorující komunikace mohou mít rovněž nepříznivé účinky na základní práva zaměstnanců sdružovat se, pořádat setkání pracovníků a důvěrně komunikovat (včetně práva získávat informace). Monitorování komunikací a chování bude na zaměstnance vyvíjet tlak, aby se přizpůsobili a předešli tak tomu, že by se zjistilo něco, co může být vnímáno jako anomálie, a to způsobem srovnatelným s tím, jak intenzivní používání průmyslových kamer ovlivnilo chování lidí ve veřejném prostoru. Vzhledem ke schopnostem těchto technologií si zaměstnanci kromě toho nemusí být vědomi, jaké osobní údaje jsou zpracovávány a pro jaké účely, přičemž si dokonce nemusí být vědomi ani existence samotné monitorovací technologie.

Používaní monitorovací informační technologie se rovněž liší od jiných viditelnějších nástrojů pro pozorování a monitorování, jako jsou například průmyslové kamery, protože k němu může docházet tajně. Jestliže neexistuje snadno srozumitelná a přístupná politika monitorování pracoviště, zaměstnanci si nemusí být vědomi existence a důsledků probíhajícího monitorování, a proto nemohou uplatňovat svá práva. Další riziko pramení z „nadměrného shromažďování“ údajů v těchto systémech, např. v systémech shromažďujících lokalizační údaje prostřednictvím WiFi.

Nárůst množství údajů získaných v prostředí pracoviště v kombinaci s novými technikami pro analýzu údajů a křížovou kontrolu rovněž může vytvořit rizika neslučitelného dalšího zpracování. Příklady nelegitimního dalšího zpracování zahrnují používání systémů, které jsou legitimně instalovány k ochraně majetku, k monitorování dostupnosti a výkonu zaměstnanců a jejich vstřícnosti vůči zákazníkům. Jako další příklad lze uvést používání údajů shromážděných prostřednictvím systému průmyslových kamer k pravidelnému monitorování chování a výkonu zaměstnanců, nebo používání údajů ze systému určujícího zeměpisnou polohu (jako např. monitorování prostřednictvím WiFi nebo Bluetooth) k neustálé kontrole pohybu a chování zaměstnanců.

V důsledku toho může toto monitorování zasahovat do práv zaměstnanců na soukromí, a to bez ohledu na to, zda k monitorování dochází systematicky nebo příležitostně. Riziko není omezeno pouze na analýzu obsahu komunikací. Analýza metadat o určité osobě může umožnit podrobné monitorování života a vzorců chování fyzické osoby, které narušuje soukromí ve stejné míře.

Rozsáhlé využívání monitorovacích technologií rovněž může snížit ochotu zaměstnanců (a omezit kanály, jejichž prostřednictvím by mohli) informovat zaměstnavatele o nesrovnalostech nebo nezákonném jednání nadřízených a/nebo jiných zaměstnanců, u kterých hrozí, že by mohly poškodit podnikání (zejména údaje o klientech) nebo pracoviště. K tomu, aby dotčený zaměstnanec začal jednat a takové situace ohlásil, je často třeba anonymita. Monitorování, které zasahuje do práv zaměstnanců na soukromí, může narušit nezbytnou komunikaci s příslušnými pracovníky. V takovém případě mohou zavedené prostředky, jak

mohou oznamovatelé z řad zaměstnanců (tzv. whistlebloweři) hlásit podezření z protiprávního jednání, ztratit efektivitu[14].

5. Scénáře

Tento oddíl se zabývá řadou scénářů zpracování údajů na pracovišti, v nichž nové technologie a/nebo rozvoj stávajících technologií mají, nebo mohou mít, potenciál k tomu, že vysoce ohrozí soukromí zaměstnanců. Ve všech takových případech by zaměstnavatelé měli zvážit, zda je:

- činnost zpracování nezbytná, a pokud ano, který právní základ se uplatní,
- navrhované zpracování osobních údajů spravedlivé vůči zaměstnancům,
- činnost zpracování přiměřená vzneseným obavám a
- činnost zpracování transparentní.

5.1 Operace zpracování během náborového procesu

Používání sociálních médií fyzickými osobami je všeobecně rozšířené a je poměrně běžné, že uživatelské profily jsou veřejně viditelné, v závislosti na nastavení zvoleném držitelem účtu. V důsledku toho se zaměstnavatelé mohou domnívat, že kontrola profilů případných uchazečů na sociálních sítích během náborového procesu může být odůvodněna. Toto může platit i pro další veřejně dostupné informace o potenciálním zaměstnanci.

Zaměstnavatelé by však neměli předpokládat, že mohou zpracovávat tyto údaje pro své vlastní účely pouze proto, že profil fyzické osoby na sociálních médiích je veřejně dostupný. Pro toto zpracování je vyžadován právní základ, jako například oprávněný zájem. V této souvislosti by zaměstnavatel měl – před kontrolou profilu na sociálních médiích – zohlednit, zda profil žadatele na sociálních médiích souvisí s obchodními nebo soukromými účely, jelikož se může jednat o důležité vodítko pro právní přípustnost kontroly údajů. Kromě toho mohou zaměstnavatelé shromažďovat a zpracovávat osobní údaje uchazečů o zaměstnání pouze v rozsahu, v jakém je shromažďování těchto údajů nezbytné a důležité pro výkon zaměstnání, o které se daná osoba uchází.

Obecně platí, že údaje shromážděné během náborového procesu by měly být smazány, jakmile je zřejmé, že nabídka zaměstnání nebude dotčené fyzické osobě učiněna, nebo že ji tato osoba nepřijme[15]. Fyzická osoba rovněž musí být o veškerém takovém zpracování řádně informována ještě před tím, než se zapojí do náborového procesu.

---

[14] Viz například pracovní skupina WP29, *stanovisko č. 1/2006 k problematice užívání právních předpisů EU o ochraně údajů na vnitřní postupy oznamování podezření z protiprávního jednání (whistleblowing) v oblasti účetnictví, vnitřních účetních kontrol, záležitostí auditu, boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru*, WP 117, 1. února 2006, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_cs.pdf

[15] Viz také Rada Evropy, *doporučení Výboru ministrů Rady Evropy členským státům č. CM/Rec (2015) ohledně zpracování osobních údajů v souvislosti se zaměstnáním*, odstavec 13.2 (1. dubna 2015, internetová stránka: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). V případech, kdy si zaměstnavatel s ohledem na další pracovní příležitosti přeje údaje uchovat, by o tom měl být subjekt údajů náležitě informován a měla by mu být dána možnost vznést proti tomuto dalšímu zpracování námitku, přičemž v takovém případě by měly být údaje vymazány (Id.).

Neexistuje žádný právní základ pro to, aby zaměstnavatel po potenciálních zaměstnancích požadoval, aby si jej „zařadili do přátel“, nebo aby mu jinými způsoby poskytli přístup k obsahu svých profilů.

Příklad

Během náboru nového zaměstnance zaměstnavatel zkontroluje profily uchazečů na různých sociálních sítích a informace z těchto sítí (a veškeré další informace dostupné na internetu) zahrne do procesu prověřování.

Zaměstnavatel může mít pro zkoumání veřejně dostupných informací o uchazečích právní základ podle čl. 7 písm. f), pouze je-li pro zaměstnání nezbytné přezkoumat informace o uchazeči na sociálních médiích, například aby bylo možné posoudit konkrétní rizika v souvislosti s uchazeči o konkrétní funkci, a jsou-li uchazeči řádně informováni (např. v textu pracovního inzerátu).

5.2 Operace zpracování v důsledku prověřování v zaměstnání

Prostřednictvím existence profilů na sociálních médiích a rozvoje nových analytických technologií zaměstnavatelé mají (nebo mohou získat) technické schopnosti neustále prověřovat zaměstnance, a to shromažďováním informací týkajících se jejich přátel, stanovisek, přesvědčení, zájmů, zvyků, místa pobytu, postojů a chování, a tím pádem zachycováním údajů, včetně citlivých údajů o soukromém a rodinném životě zaměstnance.

K prověřování profilů zaměstnanců na sociálních médiích v zaměstnání by nemělo docházet na všeobecném základě.

Zaměstnavatelé by se dále měli zdržet toho, aby od zaměstnance nebo uchazeče o zaměstnání požadovali přístup k informacím, které tyto osoby prostřednictvím sociálních sítí sdílejí s ostatními.

Příklad
Zaměstnavatel monitoruje profily bývalých zaměstnanců na síti LinkedIn, přičemž těmto bývalým zaměstnancům běží doba konkurenční doložky. Účelem tohoto monitorování je sledovat dodržování souladu s těmito doložkami. Monitorování je omezeno na tyto bývalé zaměstnance.

Pokud může zaměstnavatel doložit, že toto monitorování je nezbytné pro ochranu jeho oprávněných zájmů, že nejsou dostupné žádné jiné méně invazivní prostředky a že bývalí zaměstnanci byli náležitě informováni o rozsahu pravidelného sledování veřejných komunikací, pak se může opřít o právní základ čl. 7 písm. f) směrnice o ochraně údajů.

Kromě toho by se od zaměstnanců nemělo požadovat, aby používali profil na sociálních médiích, který poskytl jejich zaměstnavatel. I když se to kvůli jejich úkolům specificky předpokládá (např. mluvčí organizace), musí zaměstnancům zůstat možnost používat „nepracovní“ neveřejný profil namísto „oficiálního“ profilu zprostředkovaného zaměstnavatelem. Tento fakt by měl být upřesněn v podmínkách pracovní smlouvy.

5.3 Operace zpracování v důsledku monitorování používání IKT na pracovišti

Tradičně bylo za hlavní hrozbu pro soukromí zaměstnanců považováno monitorování elektronických komunikací na pracovišti (např. telefony, vyhledávání na internetu, e-mail, výměna rychlých zpráv (instant messaging), VOIP atd.). Pracovní skupina WP29 ve svém *pracovním dokumentu* z roku 2001 *o dohledu nad elektronickými komunikacemi na pracovišti* v souvislosti s monitorováním používání e-mailu a internetu dospěla k řadě závěrů. I když jsou tyto závěry nadále platné, je třeba zohlednit technologický rozvoj, který umožnil novější a potenciálně rušivější a všudypřítomnější způsoby monitorování. Tento rozvoj zahrnuje mimo jiné:

- nástroje zabraňující ztrátě údajů (Data Loss Prevention, DLP), které monitorují odchozí komunikace za účelem zjištění případného porušení ochrany údajů,
- firewally nové generace (Next-Generation Firewalls, NGFWs) a systémy jednotného zvládání hrozeb (Unified Threat Management, UTM), které mohou poskytnout řadu monitorovacích technologií, včetně hloubkové inspekce paketů, zachycení TLS, filtrování internetových stránek, filtrování obsahu, podávání zpráv o spotřebičích,

informací o totožnosti uživatele a (jak je popsáno výše) zabraňování ztrátě údajů. Tyto technologie mohou být v závislosti na zaměstnavateli použity i jednotlivě;

- bezpečnostní aplikace a opatření, jež zahrnují zaznamenávání přístupu zaměstnance do systémů zaměstnavatele,
- technologie eDiscovery, čímž se rozumí jakýkoliv proces vyhledávání elektronických údajů s cílem použít je jako důkaz,
- sledování, jak jsou používány aplikace a zařízení, prostřednictvím skrytého softwaru, buď na stolním počítači, nebo na cloudu,
- kancelářské aplikace poskytované jako cloudová služba používané na pracovišti, které teoreticky umožňují velmi podrobné zaznamenávání činnosti zaměstnanců,
- monitorování osobních zařízení (např. počítačů, mobilních telefonů, tabletů), která zaměstnanci používají pro svou práci na základě konkrétní politiky užívání, jako například zásady „přines si své vlastní zařízení), jakož technologie MDM (správa mobilních zařízení, *Mobile Device Management*), která umožňuje distribuci aplikací, údajů, konfiguraci nastavení a opravných příkazů pro mobilní zařízení, a
- používání nositelných zařízení (např. zařízení monitorující zdravotní stav a fyzickou kondici).

Je možné, že zaměstnavatel použije monitorovací řešení „vše v jednom“, jako například sadu bezpečnostních souborů, která mu umožní monitorovat veškeré používání IKT na pracovišti, na rozdíl od pouhého monitorování e-mailu a/nebo internetových stránek, jako tomu bylo dříve. Závěry přijaté v pracovním dokumentu WP55 se použijí na veškeré systémy umožňující, aby k takovému monitorování došlo[16].

Příklad

Zaměstnavatel má v úmyslu nasadit inspekční zařízení TLS, aby mohl dekódovat a kontrolovat bezpečný provoz, a to s cílem zjistit cokoliv škodlivého. Zařízení je rovněž schopno nahrávat a analyzovat veškerou on-line činnost zaměstnance na síti organizace.

Používání šifrovaných komunikačních protokolů je v rostoucí míře uplatňováno na ochranu on-line toků údajů obsahujících osobní údaje před zachycením. Může to však rovněž představovat problém, jelikož šifrování znemožňuje monitorovat příchozí a odchozí údaje. Inspekční zařízení TLS dekóduje datový tok, pro účely bezpečnosti zanalyzuje obsah a poté tok znovu zašifruje.

V tomto případě se zaměstnavatel opírá o oprávněný zájem – nutnost chránit síť a osobní údaje zaměstnanců a zákazníků uchovávané v rámci této sítě před neoprávněným přístupem nebo únikem dat. Monitorování veškerých on-line činností zaměstnanců však představuje nepřiměřenou reakci a zásah do práva na důvěrnost komunikací. Zaměstnavatel by měl nejprve prozkoumat jiné, méně invazivní prostředky pro ochranu důvěrnosti údajů zákazníků a bezpečnosti sítě.

[16] Viz také věc *Copland v. Spojené království*, (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ESLP 253 (internetová stránka: http://www.bailii.org/eu/cases/ECHR/2007/253.html), ve které soud uvedl, že e-maily odeslané z obchodních prostor a informace odvozené z monitorování používání internetu mohou být součástí soukromého života a korespondence zaměstnance a že shromažďování a ukládání těchto informací bez vědomí zaměstnance by představovalo zásah do práv zaměstnance. Soud však nerozhodl, že by toto monitorování nebylo v demokratické společnosti nikdy nezbytné.

V rozsahu, v jakém může být zachycení provozu TLS považováno za zcela nezbytné, by mělo být zařízení konfigurováno takovým způsobem, aby bránilo trvalému zaznamenávání činnosti zaměstnance, například blokováním podezřelého příchozího nebo odchozího toku dat a přesměrováváním uživatele na informační portál, kde uživatel může požádat o přezkoumání takového automatizovaného rozhodnutí. Pokud by nicméně některé obecné zaznamenávání bylo považováno za zcela nezbytné, lze zařízení rovněž nakonfigurovat tak, aby neukládalo zaznamenané údaje, pokud zařízení nesignalizuje výskyt incidentu. Shromažďované údaje by přitom měly být minimalizovány.

Jakožto osvědčený postup by zaměstnavatel mohl nabídnout zaměstnancům alternativní nemonitorovaný přístup. Může to být formou nabídnutí volné sítě WiFi nebo samostatných zařízení či terminálů (s odpovídajícími zárukami pro zajištění důvěrnosti komunikací), kde mohou zaměstnanci uplatňovat své legitimní právo používat pracovní vybavení pro určité soukromé využití[17]. Zaměstnavatelé by dále měli posoudit určité druhy provozu, jejichž zachycování ohrožuje řádnou rovnováhu mezi jejich oprávněnými zájmy a soukromím zaměstnance – jako například používání soukromého e-mailového účtu či on-line bankovnictví a návštěvy internetových stránek o zdraví –, a to s cílem vhodně nakonfigurovat zařízení tak, aby nepokračovalo v zachycování komunikací za okolností, které nejsou v souladu s proporcionalitou. Zaměstnanci by měli mít přesné informace o tom, jaký druh komunikace zařízení monitoruje.

Měla by být vypracována pravidla, za jakých okolností a kdo může mít přístup k podezřelým zaznamenaným údajům, a tato pravidla by měla být snadno a trvale přístupná všem zaměstnancům, aby jim rovněž mohla sloužit jako průvodce pro přijatelné a nepřijatelné používání sítě a vybavení. To zaměstnancům umožňuje upravit své chování a předejít tomu, aby byli monitorováni při oprávněném používání pracovního informačního vybavení pro soukromé účely. Jakožto osvědčený postup by tato pravidla měla být alespoň jednou ročně vyhodnocena, aby se posoudilo, zda zvolené monitorovací řešení přináší zamýšlené výsledky a zda pro dosažení stejných účelů existují jiné, méně invazivní nástroje nebo prostředky.

Bez ohledu na dotčenou technologii nebo schopnosti, kterými tato technologie disponuje, lze právní základ podle čl. 7 písm. f) použít pouze tehdy, splňuje-li zpracování určité podmínky. Zaprvé, zaměstnavatelé používající tyto produkty a aplikace musí zvážit proporcionalitu opatření, která provádějí, a také to, zda je možné přijmout nějaká další opatření, která by zmírnila nebo snížila rozsah a dopad zpracování údajů. Jakožto příklad osvědčeného postupu by toto zvážení mohlo mít formu posouzení vlivu na ochranu osobních údajů provedeného před zavedením jakékoliv monitorovací technologie. Zadruhé, zaměstnavatelé musí uplatňovat pravidla přijatelného používání spolu s pravidly na ochranu soukromí, přičemž popíší přípustné používání sítě a vybavení organizace a důrazně a podrobně uvedou, k jakému zpracování dochází. O těchto pravidlech musí také zaměstnance informovat.

V některých zemích by vytvoření takových pravidel právně vyžadovalo schválení radou zaměstnanců nebo podobným orgánem reprezentujícím zaměstnance. V praxi taková pravidla

[17] Viz věc *Halford v. Spojené království* [1997] ESLP 32, (internetová stránka: http://www.bailii.org/eu/cases/ECHR/1997/32.html), ve které soud uvedl, že „na telefonické hovory uskutečněné z obchodních prostor, jakož i z domova se mohou vztahovat pojmy „soukromý život“ a „korespondence“ ve smyslu čl. 8 odst. 1 [Úmluvy]“ a věc *Barbulescu v. Rumunsko*, [2016] ESLP 61, (internetová stránka: http://www.bailii.org/eu/cases/ECHR/2016/61.html), týkající se používání pracovního účtu pro výměnu rychlých zpráv pro osobní korespondenci, v níž soud uvedl, že monitorování účtu zaměstnavatelem bylo omezené a přiměřené; odlišné stanovisko soudce Pinta de Alberquerque, který se zasazoval o nastolení pečlivé rovnováhy.

často vypracovávají pracovníci údržby IT. Vzhledem k tomu, že tito pracovníci se budou zaměřovat především na bezpečnost, a nikoliv na oprávněná očekávání zaměstnanců týkající se soukromí, pracovní skupina WP29 doporučuje, aby byl do posuzování nutnosti monitorování, jakož i logiky těchto pravidel a jejich dostupnosti ve všech případech zapojen reprezentativní vzorek zaměstnanců.

Příklad

Zaměstnavatel nasadí nástroj zabraňující ztrátě údajů (DLP), aby automaticky monitoroval odchozí e-maily. Účelem je zabránit neoprávněnému přenesení údajů, které jsou předmětem průmyslového vlastnictví (např. osobní údaje zákazníků), nezávisle na tom, zda je tato činnost neúmyslná, či nikoliv. Jakmile je e-mail považován za potenciální zdroj porušení ochrany údajů, provede se další šetření.

Zaměstnavatel opět spoléhá na nezbytnost svého oprávněného zájmu chránit osobní údaje zákazníků, jakož i svá aktiva před neoprávněným přístupem nebo únikem dat. Tento nástroj DLP však může zahrnovat zpracování osobních údajů, které není nezbytné – například „falešně pozitivní“ poplach může vést k neoprávněnému přístupu k legitimním e-mailům, které zaměstnanci odeslali (může se například jednat např. o osobní e-maily).

Nezbytnost nástroje DLP a jeho nasazení by proto měla být plně odůvodněna, aby byla nastolena řádná rovnováha mezi oprávněnými zájmy zaměstnavatele a základním právem na ochranu osobních údajů zaměstnanců. Aby bylo možné opřít se o oprávněné zájmy zaměstnavatele, měla by být přijata určitá opatření na zmírnění rizik. Například pravidla, podle kterých systém postupuje při charakterizování e-mailu jakožto případného porušení ochrany údajů, musí být pro uživatele plně transparentní, a v případech, kdy nástroj rozezná e-mail, který má být odeslán, jakožto možné porušení ochrany údajů, by měl být odesílatel e-mailu před jeho přenesením informován prostřednictvím varovné zprávy, aby tak měl možnost toto přenesení zrušit.

V některých případech je monitorování zaměstnanců možné nikoli kvůli nasazení specifických technologií, ale jednoduše proto, že se očekává, že zaměstnanci budou používat on-line aplikace poskytnuté zaměstnavatelem, které umožňují zpracování osobních údajů. Příkladem je používání kancelářských aplikací založených na cloudu (např. textových editorů, kalendářů, sociálních sítí). Je třeba zajistit, aby si zaměstnanci mohli vyhradit určitá soukromá místa, k nimž může zaměstnavatel získat přístup pouze za výjimečných okolností. To platí například pro kalendáře, které jsou často používány pro soukromé schůzky. Pokud si zaměstnanec schůzku nastaví jako „soukromou“, nebo to poznamená do samotné schůzky, zaměstnavateli (a ostatním zaměstnancům) by nemělo být umožněno přezkoumávat obsah schůzky.

Požadavek subsidiarity v této souvislosti někdy znamená, že nelze provádět žádné monitorování. Je tomu tak například tehdy, kdy lze zakázanému používání komunikačních služeb předejít zablokováním určitých internetových stránek. Pokud je možné zablokovat internetové stránky, mělo by být za účelem dodržování požadavku subsidiarity namísto nepřetržitého monitorování veškerých komunikací zvoleno zablokování.

Obecněji platí, že na prevenci by měl být kladen mnohem větší důraz než na detekci – pro zájmy zaměstnavatele je lepší předcházet zneužívání internetu technickými prostředky než vynakládáním zdrojů na zjišťování zneužívání.

5.4 Operace zpracování v důsledku monitorování používání IKT mimo pracoviště

Používání IKT mimo pracoviště začalo být s růstem politik práce z domu, práce na dálku a politiky založené na zásadě „přines si své vlastní zařízení“ mnohem běžnější. Schopnosti těchto technologií mohou představovat riziko pro soukromý život zaměstnanců, jelikož

monitorovací systémy existující na pracovišti se v řadě případů, fakticky rozšiřují do domácí sféry zaměstnanců, pokud zaměstnanci takováto zařízení používají.

5.4.1 *MONITOROVÁNÍ PRÁCE Z DOMOVA A PRÁCE NA DÁLKU*

Začalo být mnohem běžnější, že zaměstnavatelé svým zaměstnancům nabízejí možnost práce na dálku, např. z domova a/nebo při přesunech. Toto je ústřední faktor stojící za stíráním rozdílu mezi pracovištěm a domovem. Obecně to znamená, že v závislosti na konkrétním provedení zaměstnavatel vydá zaměstnancům IKT zařízení nebo software, který jim po nainstalování v jejich domově / na jejich vlastních zařízeních umožní mít přístup k síti, systémům a zdrojům zaměstnavatele na stejné úrovni, jako by se nacházeli na pracovišti.

Ačkoliv práce na dálku může představovat pozitivní vývoj, jedná se rovněž o oblast dalšího rizika pro zaměstnavatele. Například zaměstnanci, kteří mají vzdálený přístup k infrastruktuře zaměstnavatele, nejsou vázáni fyzickými bezpečnostními opatřeními, která mohou být zavedena v prostorách zaměstnavatele. Jednoduše řečeno: bez zavedení vhodných technických opatření se riziko neoprávněného přístupu zvyšuje a může vést ke ztrátě nebo zničení informací, které mohou být v držení zaměstnavatele, a to včetně osobních údajů zaměstnanců nebo zákazníků.

Zaměstnavatelé, kteří chtějí zmírnit rizika v této oblasti, se mohou domnívat, že existuje důvod pro nasazení softwarových balíčků (buď na místě, nebo na cloudu), které například dokážou zaznamenávat údery na klávesnici nebo pohyby myší, pořizovat snímky obrazovky (buď náhodně, nebo ve stanovených intervalech), zaznamenávat použité aplikace (jak dlouho byly používány) a, u kompatibilních zařízení, spouštět webové kamery a shromažďovat jejich videozáznamy. Tyto technologie jsou široce dostupné, a to i od třetích stran, jako jsou například poskytovatelé cloudů.

Zpracování údajů jako součást těchto technologií je však nepřiměřené a je velmi nepravděpodobné, že by zaměstnavatel mohl jako právní základ použít oprávněný zájem, např. pro zaznamenávání úderů na klávesnici nebo pohybů myší zaměstnance.

Klíčové je řešit riziko představované prací z domova a prací na dálku přiměřeným, a nikoliv neúměrným způsobem, ať už se tato možnost nabízí jakýmikoli prostředky a bez ohledu na to, jaká technologie je navrhována, a to zejména jsou-li hranice mezi pracovním a soukromým použitím proměnlivé.

5.4.2 *ZÁSADA „PŘINES SI SVÉ VLASTNÍ ZAŘÍZENÍ“*

Vzhledem k rostoucí oblíbenosti a zlepšování funkcí a schopností spotřebních elektronických zařízení mohou zaměstnanci požadovat na zaměstnavateli, aby jim k výkonu práce na pracovišti umožnil používat jejich vlastní zařízení. Toto je známo jako zásada „přines si své vlastní zařízení“.

Účinné provádění tohoto přístupu může mít pro zaměstnance řadu výhod, včetně zlepšení pracovní spokojenosti, celkového zlepšení morálky, zvýšení účinnosti práce a větší flexibility. Z definice však bude zaměstnanec někdy používat zařízení k osobním účelům, což je pravděpodobné zejména v určité časy (např. večery, víkendy). Existuje proto zřetelná možnost, že skutečnost, že zaměstnanci používají vlastní zařízení, povede k tomu, že zaměstnavatelé budou zpracovávat informace o těchto zaměstnancích a případně o jakýchkoliv rodinných příslušnících, kteří toto zařízení nepatřící podniku používají také.

V souvislosti se zaměstnáním jsou rizika pro soukromí způsobená uplatňováním zásady „přines si své vlastní zařízení“ obvykle spojena s monitorovacími technologiemi shromažďujícími identifikátory, jako například fyzické adresy MAC, nebo s případy, kdy zaměstnavatel vstoupí do zařízení zaměstnance s odůvodněním, že provádí bezpečnostní kontrolu, tj. zjišťování škodlivého softwaru (malware). Pokud jde o druhý uvedený případ, existuje řada komerčních řešení umožňujících prohlížení soukromých zařízení, jejich použitím je však možné potenciálně získat přístup k veškerým údajům na tomto zařízení, a proto je třeba je pečlivě spravovat. Například ty části zařízení, u nichž se předpokládá, že budou použity pouze pro soukromé účely (např. složka na ukládání fotografií pořízených daných zařízením) v zásadě nemohou být přístupné.

Monitorování umístění a provozu na těchto zařízeních může být považováno za sloužící oprávněnému zájmu chránit osobní údaje, za něž je zaměstnavatel jakožto správce údajů odpovědný. Jedná-li se však o osobní zařízení zaměstnance, může být tento postup protiprávní, pokud takové monitorování zachycuje rovněž údaje související se soukromým a rodinným životem zaměstnance. Aby se předešlo monitorování soukromých informací, musí být zavedena vhodná opatření umožňující rozlišovat mezi soukromým a pracovním používáním zařízení.

Zaměstnavatelé by rovněž měli zavést metody, jejichž prostřednictvím budou jejich vlastní údaje v daném zařízení bezpečně přenášeny mezi tímto zařízením a jejich sítí. Může se stát, že zařízení je proto konfigurováno tak, aby k zajištění určité úrovně bezpečnosti směřovalo veškerý tok dat prostřednictvím VPN zpět do podnikové sítě. Pokud je však takové opatření použito, zaměstnavatel by měl rovněž zvážit, že software instalovaný pro účely monitorování během doby, kdy je zařízení zaměstnancem používáno pro osobní účely, představuje riziko ohrožení soukromí. Mohou být použita zařízení nabízející další ochranu, jako například tzv. „sandboxing“ údajů (uchovávání údajů ve zvláštní aplikaci).

Naopak, pokud neexistuje žádný způsob, jak zabránit monitorování soukromého používání, musí zaměstnavatel rovněž zvážit, zda používání konkrétních pracovních zařízení pro soukromé účely nezakázat – například pokud zařízení nabízí vzdálený přístup k osobním údajům, pro které je zaměstnavatel správcem údajů.

5.4.3 *SPRÁVA MOBILNÍCH ZAŘÍZENÍ*

Správa mobilních zařízení (*mobile device management*, MDM) zaměstnavatelům umožňuje na vyžádání vzdáleně zjistit polohu zařízení, nastavit specifické konfigurace a/nebo aplikace a mazat údaje. Zaměstnavatel může tuto funkci ovládat sám, nebo k tomu může použít třetí stranu. Služby MDM zaměstnavatelům rovněž umožňují nahrávat nebo sledovat zařízení v reálném čase, a to i tehdy, když není nahlášeno jako kradené.

Pokud je takováto technologie nová, nebo pokud ji správce údajů používá nově, mělo by být před jejím nasazením provedeno posouzení vlivu na ochranu osobních údajů. Pokud z tohoto posouzení vyplyne, že technologie MDM je za zvláštních okolností nezbytná, stále je třeba provést posouzení, zda je výsledné zpracování údajů v souladu se zásadami subsidiarity a proporcionality. Zaměstnavatelé musí zajistit, aby údaje shromážděné v rámci funkce vzdáleného zjišťování polohy byly zpracovány pro stanovený účel a netvořily, a ani nemohly tvořit, součást širšího programu umožňujícího průběžné sledování zaměstnanců. Funkce sledování by měly být omezeny i pro stanovený účel. Sledovací systémy mohou být navrženy tak, aby zaznamenávaly lokalizační údaje, aniž by je předávaly zaměstnavateli – za takových

okolností by lokalizační údaje měly být k dispozici pouze v případech, kdy by došlo k nahlášení zařízení nebo k jeho ztrátě.

Zaměstnanci, jejichž zařízení jsou přihlášena ke službám MDM, musí být rovněž plně informováni o tom, jaké sledování probíhá a jaké to pro ně má důsledky.

5.4.4 *NOSITELNÁ ZAŘÍZENÍ*

Zaměstnavatelé jsou ve stále větším pokušení poskytnout svým zaměstnancům nositelná zařízení, aby mohli sledovat a monitorovat jejich zdravotní stav a činnost na pracovišti, a někdy dokonce i mimo něj. Toto zpracování údajů však zahrnuje zpracování údajů o zdravotním stavu, a proto je na základě článku 8 směrnice o ochraně údajů zakázáno.

Vzhledem k nerovnému vztahu mezi zaměstnavateli a zaměstnanci – tj. zaměstnanec je na zaměstnavateli finančně závislý – a citlivé povaze údajů o zdravotním stavu je vysoce nepravděpodobné, že pro sledování nebo monitorování těchto údajů lze udělit právně platný výslovný souhlas, jelikož zaměstnanci v první řadě v podstatě nemají „svobodu“ takovýto souhlas udělit. I kdyby zaměstnavatel ke shromažďování údajů o zdravotním stavu používal třetí stranu, která by mu poskytovala pouze souhrnné informace o jeho obecném vývoji, zpracování by stále bylo protiprávní.

Rovněž, jak je popsáno ve *stanovisku č. 5/2014 k technikám anonymizace*[18], je technicky velmi obtížné zajistit úplnou anonymizaci údajů. Dokonce i v prostředí s více než tisíci zaměstnanci by byl zaměstnavatel vzhledem k dostupnosti jiných údajů o zaměstnancích stále schopen vyčlenit jednotlivé zaměstnance s konkrétními zdravotními indikacemi, jako například vysoký krevní tlak nebo obezita.

Příklad:

Organizace svým zaměstnancům nabídne jako všeobecný dárek zařízení sledující fyzickou kondici. Zařízení počítá počet kroků, které zaměstnanci ujdou, a v průběhu doby zaznamenává jejich puls a spánkové vzorce.

Výsledné údaje o zdravotním stavu by měly být přístupné pouze zaměstnanci, nikoliv zaměstnavateli. Jakékoliv údaje přenesené mezi zaměstnancem (jakožto subjektem údajů) a poskytovatelem zařízení/služby (jakožto správcem údajů) mají být přístupné pouze těmto stranám.

Jelikož údaje o zdravotním stavu mohou být rovněž zpracovávány komerční stranou, která zařízení vyrobila nebo která zaměstnavatelům nabízí služby, zaměstnavatel by měl při volbě zařízení nebo služby zhodnotit politiku ochrany soukromí výrobce a/nebo poskytovatele služeb a zajistit, že nedochází k nezákonnému zpracování údajů o zdravotním stavu zaměstnanců.

5.5 Operace zpracování související s časem a docházkou

Systémy umožňující zaměstnavatelům kontrolovat, kdo může vstoupit do jejich prostor a/nebo určitých míst v rámci jejich prostor, mohou rovněž umožňovat sledování činností

[18] Pracovní skupina WP29, *stanovisko č. 5/2014 k technikám anonymizace*, WP 216, 10. dubna 2014, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_cs.pdf

zaměstnanců. Ačkoliv takovéto systémy existují již řadu let, stále více jsou nasazovány nové technologie ke sledování času a docházky zaměstnanců, a to včetně systémů zpracovávajících biometrické údaje i jiných systémů, jako např. sledování mobilních zařízení.

Ačkoliv tyto systémy mohou tvořit důležitou složku auditní stopy zaměstnavatele, představují rovněž riziko, že poskytnou nadměrné množství informací o činnosti zaměstnance během přítomnosti na pracovišti a umožní v této souvislosti kontrolu.

Příklad:

Zaměstnavatel spravuje serverovnu, v níž jsou v digitální podobě uloženy citlivé obchodní informace, osobní údaje zaměstnanců a osobní údaje zákazníků. Za účelem splnění právní povinnosti zabezpečit údaje proti neoprávněnému přístupu zaměstnavatel nainstaloval systém kontroly přístupu, který zaznamenává příchod a odchod zaměstnanců, kteří mají příslušné povolení vstoupit do místnosti. Pokud by se nějaká součást vybavení ztratila, nebo pokud by se jakékoliv údaje staly předmětem neoprávněného přístupu, ztráty nebo krádeže, záznamy uchovávané zaměstnavatelem umožní určit, kdo měl v dané době do místnosti přístup.

Vzhledem k tomu, že zpracování je nezbytné a nepřevažuje nad právem zaměstnanců na soukromý život, může se jednat o oprávněný zájem podle čl. 7 písm. f), pokud byli zaměstnanci o operaci zpracování náležitě informováni. Nepřetržité monitorování četnosti a přesných časů příchodu a odchodu zaměstnanců však nemůže být odůvodněno, jsou-li tyto údaje používány rovněž pro jiný účel, jako například hodnocení výkonnosti zaměstnance.

5.6 Operace zpracování používající videosystémy monitorování

Videosystémy pro monitorování a dohled, které umožňují nepřetržitě zachycovat chování pracovníka, nadále představují podobné problémy pro soukromí zaměstnanců jako dříve[19]. Nejvýznamnější změny v používání této technologie v souvislosti se zaměstnáním jsou schopnost snadno získat vzdálený přístup ke shromážděným údajům (např. prostřednictvím chytrého telefonu), zmenšení velikosti kamer (spolu se zvýšením jejich schopností, např. vysoké rozlišení) a skutečnost, že zpracování může být provedeno pomocí nové videoanalytiky.

Díky schopnostem videoanalytiky může zaměstnavatel automatizovanými prostředky mimo jiné monitorovat výrazy obličeje pracovníka, aby identifikoval odchylky od předem definovaných vzorců pohybu (např. v prostředí továren). Toto by bylo nepřiměřené vůči právům a svobodám zaměstnanců, a proto obecně protiprávní. Je rovněž pravděpodobné, že toto zpracování by zahrnovalo profilování a případně automatizované rozhodování. Zaměstnavatelé se by proto měli zdržet používání technologií umožňujících rozpoznávání obličeje. Mohou existovat určité okrajové výjimky z tohoto pravidla, takové scénáře však nemohou být použity pro uplatnění obecné legitimizace používání této technologie[20].

5.7 Operace zpracování v souvislosti s vozidly používanými zaměstnanci

[19] Viz výše uvedená věc *Köpke v. Německo*; dále je také třeba poznamenat, že v některých jurisdikcích bylo rozhodnuto, že instalování systémů, jako jsou například průmyslové kamery, je pro účel prokázání protiprávního jednání přípustné. viz věc *Bershka* u Ústavního soudu Španělska.

[20] Kromě toho podle obecného nařízení o ochraně osobních údajů musí být zpracování biometrických údajů pro účely identifikace založeno na výjimce stanovené v čl. 9 odst. 2.

Technologie umožňující zaměstnavatelům monitorovat vozidla začaly být široce používány, zejména v organizacích, jejichž činnosti zahrnují dopravu nebo které mají rozsáhlý vozový park.

Jakýkoliv zaměstnavatel používající telematiku vozidel bude shromažďovat údaje o vozidle i o konkrétním zaměstnanci, který toto vozidlo používá. Tyto údaje mohou zahrnovat nejen polohu vozidla (a tedy i zaměstnance) získanou prostřednictvím základních sledovacích systémů GPS, ale v závislosti na dané technologii také velké množství jiných informací včetně chování řidiče. Určité technologie mohou umožňovat rovněž nepřetržité monitorování vozidla i řidiče (např. zařízení pro záznam údajů o událostech).

Zaměstnavatel může být povinen instalovat sledovací technologii do vozidla, aby prokázal splnění dalších právních povinností, např. zajistit bezpečnost zaměstnanců, kteří tato vozidla řídí. Zaměstnavatel rovněž může mít oprávněný zájem na tom, aby byl schopen vozidla kdykoliv lokalizovat. I kdyby zaměstnavatelé měli oprávněný zájem dosáhnout těchto účelů, mělo by být nejprve posouzeno, zda je zpracování pro tyto účely nezbytné a zda je faktické používání těchto technologií v souladu se zásadami proporcionality a subsidiarity. Je-li povoleno používání služebního vozidla pro soukromé účely, pak je nejdůležitějším opatřením, které může zaměstnavatel k zajištění souladu s těmito zásadami přijmout, nabídnutí možnosti vyvázat se (tzv. opt-out): zaměstnanec by v zásadě měl mít možnost sledování polohy dočasně vypnout, pokud toto vypnutí odůvodňují zvláštní okolnosti, např. návštěva lékaře. Tímto způsobem může zaměstnanec ze své vlastní iniciativy určité údaje o poloze chránit jako citlivé. Zaměstnavatel musí zajistit, že shromážděné údaje nejsou použity k nelegitimnímu dalšímu zpracování, jako např. sledování a hodnocení zaměstnanců.

Zaměstnavatel rovněž musí zaměstnance jasně informovat, že do vozidla společnosti, které zaměstnanci řídí, bylo nainstalováno sledovací zařízení, a že jejich pohyb při používání tohoto vozidla je zaznamenáván (a že – v závislosti na použité technologii – může být zaznamenáváno rovněž jejich chování při řízení. Tyto informace by měly být nejlépe výrazně zobrazeny v každém vozidle, a to v zorném poli řidiče.

Zaměstnanci mohou používat služební vozidla mimo pracovní dobu, např. pro osobní užití, a to v závislosti na konkrétních pravidlech pro používání těchto vozidel. Vzhledem k citlivosti lokalizačních údajů je nepravděpodobné, že by existoval právní základ pro monitorování polohy vozidel zaměstnanců mimo dohodnutou pracovní dobu. Pokud však taková potřeba existuje, mělo by být zváženo zavedení takové technologie, které by bylo přiměřené rizikům. To může například znamenat, že by poloha vozidla, normálně zaznamenávána za účelem zabránění krádeži vozidla, nebyla registrována mimo pracovní dobu, ledaže by vozidlo opustilo široce definovaný okruh (region nebo dokonce celou zemi). Kromě toho by poloha byla zobrazena pouze při vniknutí do vozidla – zaměstnavatel by aktivoval zobrazování polohy a získal přístup k údajům, které jsou systémem již uloženy, pouze pokud by vozidlo opustilo předem definovanou oblast.

Jak je uvedeno ve *stanovisku* pracovní skupiny WP29 *č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení*[21]:

[21] Pracovní skupina WP29, *stanovisko č. 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení*, WP 185, 16. května 2011, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_cs.pdf

„Zařízení ke sledování vozidel nejsou zařízeními pro sledování zaměstnanců. Jejich funkcí je sledování nebo monitorování lokalizace vozidel, ve kterých jsou instalována. Zaměstnavatelé by je neměli považovat za zařízení ke sledování nebo monitorování chování či místa výskytu řidičů nebo jiných zaměstnanců, například zasíláním upozornění na rychlost vozidla.“

Dále, jak je uvedeno ve *stanovisku 5/2005 pracovní skupiny 29 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou*[22]:

„Zpracování lokalizačních údajů může být odůvodněné v případech, kdy slouží pro monitorování přepravy osob či zboží nebo k lepší distribuci zdrojů u služeb v rozptýlených lokalitách (např. pro plánování operací v reálném čase), nebo v případech, kdy je účelem bezpečnost samotného zaměstnance nebo jemu svěřeného zboží či vozidel. Pracovní skupina naopak považuje zpracování údajů za nadbytečné v případech, kdy si mohou zaměstnanci své cesty volně organizovat dle vlastního uvážení, nebo v případech, kdy je účelem zpracování údajů pouze sledování práce zaměstnance, která by mohla být sledována jiným způsobem.“

5.7.1 ZAŘÍZENÍ PRO ZÁZNAM ÚDAJŮ O UDÁLOSTECH

Zařízení pro záznam údajů o událostech poskytuje zaměstnavateli technickou schopnost zpracovávat významné množství osobních údajů o zaměstnancích, kteří řídí vozidla společnosti. Tato zařízení jsou do vozidel stále častěji umísťována s cílem nahrát video v případě nehody, případně včetně zvukového záznamu. Tyto systémy mohou pořizovat záznamy v určitý okamžik, např. v reakci na náhlé brždění, náhlou změnu směru nebo na nehodu, kdy jsou ukládány okamžiky bezprostředně předcházející nehodě, ale mohou být rovněž nastaveny na nepřetržité monitorování. Tyto informace mohou být následně použity k pozorování a přezkumu chování fyzické osoby při řízení s cílem toto chování zlepšit. Kromě toho řada těchto systémů obsahuje GPS pro sledování polohy vozidla v reálném čase; k dalšímu zpracování mohou být ukládány i jiné podrobné informace o řízení (např. rychlost vozidla).

Tato zařízení se rozšířila zejména mezi organizacemi, jejichž činnosti zahrnují dopravu nebo které mají významné vozové parky. Nasazení zařízení pro záznam údajů o událostech však může být zákonné, pouze pokud existuje nutnost zpracovat následné osobní údaje o zaměstnanci za oprávněným účelem, a pokud je zpracování v souladu se zásadami proporcionality a subsidiarity.

Příklad

Přepravní společnost vybaví veškerá svá vozidla videokamerou umístěnou uvnitř kabiny, která zaznamenává zvuk a obraz. Účelem zpracování těchto údajů je zlepšit řidičské dovednosti zaměstnanců. Kamery jsou nakonfigurovány tak, aby uchovávaly záznamy, kdykoliv dojde k incidentu, jako např. k náhlému zabrzdění nebo náhlé změně směru. Společnost předpokládá, že má právní základ pro zpracování v podobě jejího oprávněného zájmu podle čl. 7 písm. f) směrnice, tedy chránit bezpečnost svých zaměstnanců a dalších řidičů.

[22] Pracovní skupina WP29, *stanovisko 5/2005 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou*, WP 115, 25. listopadu 2005, internetová stránka: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_cs.pdf

Oprávněný zájem společnosti monitorovat řidiče však nemá přednost před právy těchto řidičů na ochranu jejich osobních údajů. Nepřetržité monitorování zaměstnanců těmito kamerami představuje závažný zásah do jejich práva na soukromí. Pro předcházení dopravním nehodám vozidel existují jiné a potenciálně vhodnější metody (např. instalace zařízení bránícího používání mobilních telefonů), jakož i jiné bezpečnostní systémy, jako např. vyspělé systémy nouzového brzdění nebo systémy varování při vybočení z jízdního pruhu. Kromě toho u takového videa existuje vysoká pravděpodobnost, že povede ke zpracování údajů třetích stran (jako chodců), a toto zpracování nelze dostatečně odůvodnit oprávněným zájmem společnosti.

5.8 Operace zpracování zahrnující zpřístupnění údajů o zaměstnancích třetím stranám

Začalo být stále běžnější, že společnosti za účelem zajištění spolehlivého poskytování služeb předávají údaje o svých zaměstnancích svým zákazníkům. Tyto údaje mohou být v závislosti na rozsahu poskytovaných služeb zcela nadbytečné (např. mohou obsahovat fotografii zaměstnance). Zaměstnanci však vzhledem k nerovnováze moci nejsou v postavení, kdy by mohli udělit svobodný souhlas se zpracováním svých osobních údajů zaměstnavatelem, a pokud zpracování údajů není přiměřené, zaměstnavatel nemá pro toto zpracování právní základ.

Příklad:

Doručovací společnost zašle svým zákazníkům e-mail s odkazem na jméno a polohu doručovatele (zaměstnance). Společnost má rovněž v úmyslu přiložit pasovou fotografii doručovatele. Společnost předpokládala, že bude mít právní základ pro zpracování v podobě svého oprávněného zájmu (čl. 7 písm. f) směrnice) umožnit zákazníkovi kontrolu toho, že doručovatel je skutečně ta správná osoba.

Poskytnutí jména a fotografie doručovatele zákazníkovi však není nezbytné. Vzhledem k tomu, že žádný jiný legitimní důvod pro toto zpracování neexistuje, doručovací společnost není oprávněna tyto osobní údaje zákazníkům poskytovat.

5.9 Operace zpracování zahrnující předávání personálních údajů a dalších údajů o zaměstnancích do jiné země

Zaměstnavatelé stále častěji používají aplikace a služby založené na cloudu, jako například aplikace a služby určené pro nakládání s údaji o lidských zdrojích, jakož i on-line kancelářské aplikace. Používání většiny těchto aplikací povede k předávání údajů, které se týkají zaměstnanců a které od těchto zaměstnanců pocházejí, do jiné země. Jak již bylo dříve nastíněno ve stanovisku č. 8/2001, článek 25 směrnice uvádí, že k předání osobních údajů do třetích zemí mimo EU může dojít, pouze pokud dotyčná země zajistí odpovídající úroveň ochrany. Předání by bez ohledu na základ mělo splňovat ustanovení této směrnice.

Mělo by proto být zajištěno, že tato ustanovení týkající se předávání údajů do jiné země jsou dodržována. Pracovní skupina WP29 znovu opakuje své předchozí stanovisko, že je vhodnější opírat se o odpovídající ochranu než o odchylky uvedené v článku 26 směrnice o ochraně údajů; pokud zpracování údajů probíhá na základě souhlasu, musí být tento souhlas výslovný, jednoznačný a svobodný. Mělo by však rovněž být zajištěno, že údaje sdílené mimo EU/EHP a následný přístup umožněný dalším subjektům v rámci skupiny zůstává omezený na minimální úroveň nezbytnou pro zamýšlené účely.

6. Závěry a doporučení

6.1 Základní práva

Obsah výše uvedených komunikací, jakož i údaje o provozu týkající se těchto komunikací, požívají stejnou ochranu základních práv jako „analogové“ komunikace.

Na elektronické komunikace uskutečněné z obchodních prostor se mohou vztahovat pojmy „soukromý život“ a „korespondence“ ve smyslu čl. 8 odst. 1 Evropské úmluvy. Na základě současné směrnice o ochraně údajů mohou zaměstnavatelé shromažďovat údaje pouze pro oprávněné účely, přičemž zpracování musí probíhat za vhodných podmínek (např. musí být přiměřené a nezbytné, za účelem skutečného a existujícího zájmu a provedeno zákonným, jasně formulovaným a transparentním způsobem) a pro zpracování osobních údajů shromážděných z elektronických komunikací nebo vytvořených prostřednictvím elektronických komunikací musí existovat právní základ.

Skutečnost, že zaměstnavatel vlastní elektronické prostředky, nevylučuje práva zaměstnanců na důvěrnost jejich komunikací, souvisejících údajů o poloze a korespondence. Sledování polohy zaměstnanců prostřednictvím zařízení ve vlastnictví zaměstnanců nebo prostřednictvím zařízení poskytnutých společností by mělo být omezeno na případy, kdy je zcela nezbytné pro oprávněný účel. Rozhodně platí, že v případě politiky „přines si své vlastní zařízení“ je důležité, aby zaměstnanci měli možnost chránit své soukromé komunikace před jakýmkoliv monitorováním souvisejícím se zaměstnáním.

6.2 Souhlas a oprávněný zájem

Vzhledem k závislosti vyplývající ze vztahu zaměstnavatel/zaměstnanec zaměstnanci téměř nikdy nejsou schopni svobodně udělit, odmítnout nebo zrušit souhlas. Vzhledem k nerovnováze moci mohou zaměstnanci udělit svobodný souhlas pouze za výjimečných okolností, kdy se s přijetím nebo odmítnutím nabídky nepojí žádné důsledky.

Oprávněný zájem zaměstnavatelů může být někdy uplatněn jako právní základ, ale pouze tehdy, je-li zpracování zcela nezbytné pro oprávněný účel a je-li v souladu se zásadami proporcionality a subsidiarity. Před nasazením jakéhokoliv monitorovacího nástroje by měl být proveden test přiměřenosti, aby se zvážilo, zda jsou veškeré údaje nezbytné, zda toto zpracování převažuje nad obecnými právy na soukromí, která zaměstnanci mají rovněž na pracovišti, a také to, jaká opatření musí být přijata, aby se zajistilo, že případy porušení práva na soukromý život a práva na důvěrnost komunikací jsou omezeny na nezbytné minimum.

6.3 Transparentnost

Zaměstnanci by měli být účinně informováno jakémkoli monitorování, ke kterému dochází, jeho účelech a okolnostech, za nichž probíhá, jakož i o možnostech, jak mohou zabránit tomu, aby byly jejich údaje zachycovány monitorovacími technologiemi. Politiky a pravidla týkající se oprávněného monitorování musí být jasné a snadno přístupné. Pracovní skupina doporučuje do vytváření a hodnocení těchto pravidel a politik zapojit reprezentativní vzorek zaměstnanců, jelikož většina monitorování má potenciál zasahovat do soukromých životů zaměstnanců.

6.4 Proporcionalita a minimalizace údajů

Zpracování údajů na pracovišti musí být přiměřenou reakcí na rizika, kterým zaměstnavatel čelí. Například zneužívání internetu lze zjistit, aniž by bylo nezbytné analyzovat obsah internetových stránek. Pokud lze zneužívání zabránit (např. filtrováním internetových stránek), nemá zaměstnavatel žádné obecné právo monitorovat.

Dále platí, že všeobecný zákaz komunikace pro osobní účely je nepraktický a jeho uplatňování může vyžadovat úroveň monitorování, která může být nepřiměřená. Prevenci by měla být dána mnohem větší váha než detekci – pro zájmy zaměstnavatele je lepší předcházet zneužívání internetu prostřednictvím technických prostředků než vynakládáním zdrojů na zjišťování takového zneužívání.

Informace získané z průběžného monitorování, jakož i informace, které jsou předkládány zaměstnavateli, by měly být co nejvíce minimalizovány. Zaměstnanci by měli mít možnost dočasně vypnout sledování polohy, pokud to okolnosti odůvodňují. Řešení, která například sledují vozidla, mohou být navržena tak, aby zaznamenávala údaje o poloze, aniž by je předávala zaměstnavateli.

Při rozhodování o nasazení nových technologií musí zaměstnavatelé zohlednit zásadu minimalizace údajů. Informace by měly být ukládány po minimální potřebnou dobu a doba uchovávání by měla být upřesněna. Pokud již informace nejsou dále potřebné, měly by být smazány.

6.5 Cloudové služby, on-line aplikace a předávání údajů do jiné země

Pokud se od zaměstnanců očekává používání on-line aplikací zpracovávajících osobní údaje (jako např. on-line kancelářských aplikací), zaměstnavatelé by měli zvážit možnost, že zaměstnancům umožní vyhradit určitá soukromá místa, k nimž zaměstnavatel nemůže za žádných okolností získat přístup, jako např. soukromé e-maily nebo soukromá složka s dokumenty.

Používání většiny aplikací na cloudu povede k předávání údajů o zaměstnancích do jiné země. Mělo by být zajištěno, že k předávání osobních údajů do třetí země mimo EU dojde pouze tehdy, je-li zajištěna odpovídající úroveň ochrany, a také to, že údaje sdílené mimo EU/EHP a následný přístup umožněný dalším subjektům v rámci skupiny zůstanou omezeny na minimální úroveň nezbytnou pro zamýšlené účely.

* * *

V Bruselu dne 8. června 2017

Za pracovní skupinu
předsedkyně
Isabelle FALQUE-PIERROTIN