Pracovní překlad

PRACOVNÍ SKUPINA PODLE ČLÁNKU 29

WP 249

Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti

Schváleno dne 8. června 2017

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytlo Generální ředitelství Spravedlnost a spotřebitelé Evropské Komise, B-1049 Brusel, Belgie, kancelář č. MO59 05/35.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

Obsah

1. Shrnutí

Toto stanovisko doplňuje předešlé publikace Pracovní skupiny podle článku 29 („WP29“) *Stanovisko 8/2001 ke zpracování osobních údajů v souvislosti se zaměstnáním* (WP48)[1] a *Pracovní dokument ke sledování elektronické komunikace na pracovišti* (WP55)[2] z roku 2002. Od zveřejnění těchto dokumentů se objevilo mnoho nových technologií, které umožňují systematičtější zpracování osobních údajů zaměstnanců na pracovišti, čímž přináší velké výzvy z hlediska ochrany dat a soukromí.

Toto stanovisko nově uvádí posouzení rovnováhy mezi oprávněnými zájmy zaměstnavatelů a důvodným očekáváním zaměstnanců ohledně jejich soukromí, přičemž nastiňuje rizika, která nové technologie přináší a nabízí posouzení proporcionality u řady scénářů uplatnění těchto technologií.

[1] WP29, *Stanovisko 08/2001 ke zpracování osobních údajů v souvislosti se zaměstnáním,* WP 48, 13. září 2001, url: http://ec.europa.eu/iustice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] WP29, *Pracovní dokument ke sledování elektronické komunikace na pracovišti*, WP 55, 29. května 2002, url: http://ec.europa.eu/iustice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

I když toto stanovisko vychází přednostně ze Směrnice o ochraně dat, zabývá se i novými povinnostmi, které zaměstnavatelům výhledově uloží Obecné nařízení. Opakovaně také potvrzuje názory a závěry uvedené ve stanovisku 8/2001 a pracovním dokumentu WP55, zejména tyto následující:

- Zaměstnavatelé by vždy měli pamatovat na základní zásady ochrany osobních údajů bez ohledu na použitou technologii;
- Na obsah elektronické komunikace posílané z pracovních prostor se vztahují stejná základní práva ochrany jako na komunikace analogové;
- Je vysoce nepravděpodobné, že souhlas by mohl být právním důvodem pro zpracování dat na pracovišti, ledaže by zaměstnanci měli možnost odmítnout, aniž by to pro ně mělo neblahé důsledky;
- V některých případech se lze odvolat na plnění smlouvy a oprávněné zájmy za předpokladu, že zpracování je skutečně nezbytné pro zákonné účely a je v souladu se zásadou proporcionality a subsidiarity;
- Zaměstnanci by o probíhajícím monitorování měli být účinným způsobem informováni;
- Veškeré mezinárodní přenosy zaměstnaneckých dat by měly být prováděny jen při zajištění odpovídající úrovně ochrany.

2. Úvod

Rychlé šíření nových informačních technologií, ať už jde o infrastrukturu, aplikace a chytrá zařízení, na pracovišti, umožňují nové způsoby systematického a potenciálně invazivního zpracování dat. Například:

- Technologie pro zpracování dat v práci mohou dnes být zavedeny za zlomek nákladů, než tomu bylo před několika lety, přičemž kapacita zpracování osobních údajů těmito prostředky vzrostla exponenciálně;
- Nové formy zpracování osobních údajů, kupříkladu o používání online služeb anebo lokačních údajů z chytrého zařízení, jsou pro zaměstnance mnohem méně viditelné, než jiné, tradičnější způsoby, jako třeba neskryté kamery. Vyvolává to otázku, do jaké míry mají zaměstnanci o nasazení těchto technologií povědomí, protože zaměstnavatelé by taková zpracování mohli provádět bez předchozího upozornění zaměstnanců; a
- Hranice mezi domovem a pracovištěm jsou stále nezřetelnější. Pokud třeba zaměstnanci pracují na dálku (např. z domova) nebo během služební cesty, mohou být činnosti vykonávané mimo fyzické pracovní prostory sledovány a případně to může představovat i monitorování soukromí jednotlivce.

Tyto technologie mohou pomoci při odhalování nebo prevenci škod na duševním nebo hmotném majetku firmy, při zvyšování produktivity zaměstnanců a ochraně jejich osobních údajů, za které správce nese odpovědnost, mohou však také vyvolávat vážné problémy ohledně ochrany osobních dat a soukromí. Je proto žádoucí provést nové posouzení ve věci rovnováhy mezi oprávněným zájmem zaměstnavatele ochraňovat svoji činnost a odůvodněným očekáváním subjektů údajů – zaměstnanců ohledně soukromí.

Toto stanovisko se zaměřuje nejenom na nové informační technologie v posouzení devíti různých scénářů jejich možného nasazení, ale krátce se také zabývá tradičnějšími způsoby zpracování osobních údajů na pracovišti u těch případů, kde v důsledku nových technologií došlo ke zvýšení rizika.

Slovo „zaměstnanec“ se v tomto stanovisku neomezuje úzce jen na osoby s pracovní smlouvou uzavřenou podle příslušného pracovního práva. V uplynulých dekádách se objevily různé druhy pracovního poměru sloužící novým obchodním modelům a běžnějším se stalo zejména zaměstnávání lidí na volné noze. Toto stanovisko má pokrývat všechny typy pracovního poměru, bez ohledu, zda je tento poměr založen na zaměstnanecké smlouvě.

Je důležité zmínit, že zaměstnanci, vzhledem k závislosti na zaměstnavateli vyplývající z povahy jejich vztahu, jen zřídka bývají v postavení, kdy mohou svobodně udělit souhlas, případně ho odmítnout nebo odvolat. Vyjma výjimečných situací se tedy zaměstnavatelé budou muset opírat o jiný právní důvod než souhlas – jako je třeba nutnost zpracování z důvodu oprávněného zájmu. Ani oprávněný zájem sám o sobě však nepřevažuje nad právy a svobodami zaměstnanců.

Nehledě na právní důvod by měl být ještě před zahájením zpracování proveden test proporcionality, aby se posoudilo, zda je dané zpracování k naplnění oprávněného účelu nutné, a aby se zvážila opatření nezbytná pro zajištění, že pravděpodobnost porušení práva na soukromý život a důvěrnost komunikací bude snížena na minimum. Takový test může být součástí posouzení vlivu na ochranu osobních údajů.

3. Právní rámec

Analýza v dalším textu byla provedena převážně ve vztahu ke stávajícímu právnímu rámci danému směrnicí 95/46/ES (Směrnice o ochraně dat)[3], přesto toto stanovisko zohledňuje i povinnosti podle nařízení 2016/679 (Obecné nařízení o ochraně osobních údajů“)[4], které už vstoupilo v platnost s účinností od 25. května 2018.

S ohledem na navrhované Nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích[5], vyzývá WP29 evropské zákonodárce, aby vytvořili specifickou výjimku pro sledování zařízení vydaných zaměstnancům[6]. Návrh nařízení neobsahuje vhodnou výjimku z obecného zákazu zasahování a zaměstnavatelé obvykle nemohou pořídit platný souhlas ke zpracování osobních údajů svých zaměstnanců.

3.1 Směrnice 95/46/ES — Směrnice o ochraně dat

WP29 už dříve, ve stanovisku 08/2001, sdělila, že zaměstnavatelé mají při zpracování osobních údajů v souvislosti se zaměstnáním dbát na základní zásady ochrany podle Směrnice o ochraně dat. Rozvoj nových technologií a metod zpracování na tom nic nezměnil — naopak, lze říci, že tento rozvoj učinil tento požadavek ještě naléhavějším. Zaměstnavatelé by v této souvislosti měli:

- Zajistit, aby data byla zpracována pro konkrétní a zákonné účely, jež jsou proporcionální a nezbytné;
- Pamatovat na zásadu účelového omezení a zajistit, aby údaje byly přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu;
- Uplatňovat zásady proporcionality a subsidiarity bez ohledu na uplatnitelný právní důvod;
- Být transparentní vůči zaměstnancům ohledně použití a účelů sledovacích technologií;
- Umožnit subjektům údajů výkon svých práv, včetně práva na přístup a, v náležitých případech, práva na opravu, výmaz nebo zablokování osobních údajů;
- Udržovat data přesná a neuchovávat je déle než je nutné; a
- Učinit veškerá nezbytná opatření k ochraně dat před neoprávněným přístupem a zajistit, aby si zaměstnanci byli dostatečně vědomi povinností v oblasti ochrany dat.

---

[3] 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, *Úř. věst. L 281, 23.11.1995, s. 31-50*, url: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31995L0046

[4] 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), *Úř. věst. L 119, 4.5.2016, s. 1-88*, url: 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), url: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017PC0010.

[6] Viz WP29, *Stanovisko 01/2017 k návrhu Nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích*, WP 247, 4. dubna 2017, s. 29; url: http://ec.europa.eu/newsroom/document.cfm7doc id=44103

WP29 chce vyzdvihnout, aniž by opakovala dříve poskytnutá doporučení, tři zásady, jmenovitě zákonné důvody, transparentnost a automatizovaná rozhodnutí.

3.1.1 *PRÁVNÍ DŮVODY (ČLÁNEK 7)*

Při zpracování osobních údajů v souvislosti se zaměstnáním je třeba splnit alespoň jedno z kritérií uvedených v článku 7. Pokud mezi zpracovávanými daty jsou i zvláštní kategorie údajů (podle ustanovení článku 8), je takové zpracování zakázané, neuplatní-li se výjimky[7,8].

Právní důvod podle článku 7 bude pro oprávněnost zpracování vyžadován i tehdy, pokud se zaměstnavatel může opřít o jednu z těchto výjimek.

Souhrnně řečeno, zaměstnavatelé musí věnovat pozornost následujícím konstatováním:

- 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 může být nezbytné pro **plnění smlouvy** (Článek 7 písm. b) v případech, kdy zaměstnavatel musí osobní údaje zpracovat, aby takovou povinnost splnil;
- Je zcela běžné, že **pracovní právo ukládá zákonné povinnosti** (Článek 7 písm. c)**, jež vyžadují zpracování osobních údajů;** v takových případech musí být zaměstnanec o daném zpracování jasně a plně informován (pokud se neuplatní výjimka);
- Rozhodne-li se zaměstnavatel opřít se o **oprávněný zájem** (Článek 7 písm. f), musí být účel zpracování zákonný; zvolená metoda nebo konkrétní technologie musí být nezbytná, proporcionální a uplatněná způsobem co možná nejméně dotěrným, přičemž zaměstnavatel musí být schopen prokázat, že **uplatnil náležitá opatření** k zajištění rovnováhy se základními právy a svobodami zaměstnanců[9];
- Operace zpracování musí také být ve shodě s **požadavky transparentnosti** (Články 10 a 11), a zaměstnanci by měli být jasně a plně informováni o zpracování svých údajů[10], včetně přítomnosti jakéhokoliv sledování; a
- **Náležitá technická a organizační opatření** by měla být přijata k zajištění bezpečnosti zpracování (Článek 17).

Nejdůležitější kritéria podle článku 7 jsou uvedena v dalším textu.

- **Souhlas (Článek 7 písm. a)**

Souhlas je ve Směrnici o ochraně dat definován jako jakýkoli 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 odvolatelný.

WP29 ve svém dřívějším stanovisku 8/2001 uvedla, že pokud zaměstnavatel musí osobní údaje svých zaměstnanců zpracovávat, bylo by zavádějící se domnívat, že toto zpracování může být legitimizováno zaměstnaneckým souhlasem. V případech, kdy zaměstnavatel souhlas požaduje a případný

---

[7] Jak je uvedeno v části 8 stanoviska 08/2001; článek 8 odst. 2 písm. b) například stanoví výjimku pro účely naplnění povinností a zvláštních práv správce v oblasti pracovního práva, je-li to dovoleno národním právem poskytujícím odpovídající záruky.

[8] Je potřeba uvést, že v některých zemích mají zvláštní opatření, která zaměstnavatelé musí dodržovat za účelem ochrany soukromého života zaměstnanců. Příkladem takové země je Portugalsko, kde taková zvláštní opatření existují a obdobné nástroje mohou platit i v některých dalších členských státech. Závěry uvedené v oddíle 5.6, jakož i příklady uvedené v oddílech 5.1 a 5.7.1 tohoto stanoviska, nejsou z těchto důvodů v Portugalsku platné.

[9] WP29, *Stanovisko 06/2014 k pojmu oprávněných zájmů správce podle článku 7 směrnice 95/46/ES*, WP 217, přijato 9. dubna 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

[10] Podle článku 11 odst. 2 Směrnice o ochraně dat má správce výjimku z informační povinnosti vůči subjektu údajů v případech záznamu nebo sběru dat, výslovně stanoveným zákonem.

zaměstnanců 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), pak souhlas není a ani nemůže být svobodný. Takže pro většinu případů zpracování zaměstnaneckých dat nemůže a neměl by být zaměstnanců souhlas právním důvodem, jinými slovy je nutné mít jiný právní základ.

Navíc i v případech, kdy by o souhlasu bylo možné říci, že vytváří platný právní základ zpracování (tj. pokud lze dojít k nezpochybnitelnému závěru, že tento souhlas byl udělen svobodně), musí se jednat o konkrétní a informovaný projev zaměstnancovy vůle. Přednastavení (defaultní nastavení) přístrojů a/nebo instalace softwaru, který usnadňuje elektronické zpracování osobních údajů, nemůže být považováno za souhlas udělený zaměstnancem, protože souhlas vyžaduje aktivní vyjádření vůle. Nepřítomnost aktivního úkonu (tj. neprovedení změny přednastavení) obecně nelze brát za specifický souhlas k danému zpracování[11].

- **Plnění smlouvy (Článek 7 písm. b)**

Pracovní vztahy jsou často založeny na pracovní smlouvě mezi zaměstnavatelem a zaměstnancem. Pro splnění povinností podle takové smlouvy, jako například výplata zaměstnance, musí zaměstnavatel zpracovávat některé osobní údaje.

- **Zákonné povinnosti (Článek 7 písm. c)**

Pracovní právo ukládá zaměstnavateli povinnosti, které vyžadují zpracovávat osobní údaje (např. pro účely výpočtu daní nebo mzdového účetnictví). Je jasné, že takové právo zakládá právní důvod pro zpracování dat.

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

Pokud se zaměstnavatel hodlá opřít o zákonný důvod podle článku 7 písm. f) Směrnice o ochraně dat, pak účel zpracování 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 vtíravým způsobem a být zaměřeno na specifickou rizikovou oblast. Navíc, při využití článku 7 písm. f) zůstává zaměstnanci právo na námitku vůči zpracování ze závažných a legitimních důvodů jak je stanoveno v článku 14.

Při využití článku 7 písm. f) coby právního důvodu zpracování je nezbytné přijmout zmírňující opatření, aby byla zajištěna náležitá rovnováha mezi zákonným zájmem zaměstnavatele a základními právy a svobodami zaměstnanců.[12] Taková opatření, v závislosti na formě sledování, by měla spočívat v omezení monitoringu, aby tak bylo zaručeno, že nebude narušeno soukromí zaměstnance. Takové omezení by mohlo být:

- prostorové (např. sledování jen na určitých místech; sledování citlivých prostor, třeba míst využívaných pro náboženské účely nebo sanitárních zón či šaten by mělo být zakázáno),
- datově orientované (např. osobní elektronické spisy a komunikace by neměly být sledovány), a
- časové (např. namátkové sledování namísto průběžného).

[11] Viz také WP29, *Stanovisko 15/2011 k definici souhlasu*, WP187, 13. července 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_cs.pdf

[12] Pro příklad rovnováhy, kterou je třeba nastolit viz případ *Köpke v. Německo*, [2010] ESLP 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), kdy zaměstnankyně byla propuštěna na podkladě kamerového sledování uskutečněného zaměstnavatelem a soukromou detektivní agenturou. Soud v této instanci dospěl k závěru, že národní úřady nalezly korektní rovnováhu mezi oprávněným zájmem zaměstnavatele (ochrana vlastnických práv) a právem zaměstnankyně na respektování soukromého života, jakož i veřejným zájmem na výkon spravedlnosti, současně však konstatoval, že tyto různé dotčené zájmy by v budoucnu následkem technologického rozvoje mohly nabýt různé váhy.

3.1.2 *TRANSPARENTNOST (ČLÁNKY 10 a 11)*

Požadavky na transparentnost v článcích 10 a 11 se vztahují i na zpracování dat na pracovišti; zaměstnanci musí být informováni o existenci jakéhokoli sledování, o účelech, pro které mají být osobní údaje zpracovány a musí dostat i další informace, aby zpracování bylo korektní.

S novými technologiemi je potřeba transparentnosti ještě více očividná, neboť je možné skrytě shromažďovat a dále zpracovávat ohromná množství osobních dat.

3.1.3 *AUTOMATIZOVANÁ ROZHODNUTÍ (ČLÁNEK 15)*

Článek 15 Směrnice o ochraně dat také subjektům údajů uděluje právo nebýt předmětem rozhodnutí založeného pouze na automatizovaném zpracování, které vůči nim zakládá právní účinky nebo se jich významně dotýká, a které je založeno výhradně na automatizovaném zpracování dat za účelem hodnocení určitých osobních aspektů, jako pracovní výkon, pokud takové rozhodnutí není nezbytné pro uzavření nebo plnění smlouvy v souladu s právem Unie nebo členského státu nebo není opřeno o výslovný souhlas subjektu údajů.

3.2 Nařízení 2016/679 — Obecné nařízení o ochraně osobních údajů („Obecné nařízení“)

Obecné nařízení obsahuje požadavky Směrnice o ochraně dat a dále je rozšiřuje. Pro všechny správce včetně zaměstnavatelů také zavádí nové povinnosti.

3.2.1 *ZÁMĚRNÁ OCHRANA OSOBNÍCH ÚDAJŮ*

Obecné nařízení v článku 25 vyžaduje od správců zavedení záměrné a standardní ochrany osobních údajů. Příklad: poskytuje-li zaměstnavatel svým zaměstnancům nějaké přístroje, které jsou vybaveny sledovacími technologiemi, měl by zvolit ty, jež jsou co nejšetrnější z hlediska ochrany soukromí. Vzít v úvahu je třeba také minimalizaci údajů.

3.2.2 *POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ*

Obecné nařízení v článku 35 ukládá správcům zpracovat posouzení vlivu na ochranu osobních údajů („posouzení vlivu“), 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. Příkladem je případ systematického a rozsáhlého vyhodnocování osobních aspektů jednotlivců založeného na automatizovaném zpracování včetně profilování, na základě kterého jsou činěna rozhodnutí, jež na danou fyzickou osobu mohou mít právní účinky nebo se jí obdobným způsobem významně dotýkat.

Pokud z posouzení vlivu vyplyne, že zjištěné riziko správce sám nezvládne ošetřit – tj. zbytkové riziko zůstává vysoké – pak se správce musí obrátit na dozorový úřad a konzultovat ještě před zahájením zpracování (Článek 36 odst. 1), jak je vysvětleno v pokynech WP29 k posouzení vlivu[13].

3.2.2 *„ZPRACOVÁNÍ V SOUVISLOSTI SE ZAMĚSTNÁNÍM“*

Článek 88 Obecného nařízení říká, 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 těmito účely:

- nábor;
- plnění pracovní smlouvy (včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami);

[13] WP29, *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679*, WP 248, 4. dubna 2017, url: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, s. 18.

- řízení, plánování a organizace práce;
- zajištění rovnosti a rozmanitosti na pracovišti;
- zajištění zdraví a bezpečnosti na pracovišti;
- ochrana majetku zaměstnavatele nebo majetku zákazníka;
- výkon a požívání (individuální) práv a výhod spojených se zaměstnáním; a
- ukončení zaměstnaneckého poměru.

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

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

WP29 v tomto stanovisku uvádí pokyny pro zákonné využití nových technologií v řadě konkrétních situací a podrobně probírá vhodná a zvláštní opatření k zajištění lidské důstojnosti, oprávněného zájmu a základních práv zaměstnanců.

4. Rizika

Moderní technologie 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.

Technologie sledující komunikaci mohou také mít neblahý vliv na základní práva zaměstnanců pořádat setkání pracovníků a komunikovat důvěrně (včetně práva požadovat informaci). Sledování komunikace a chování vystavuje zaměstnance tlaku přizpůsobit se, aby předešli odhalení něčeho, co by mohlo být považováno za anomálii, podobně jako intenzivní využívání kamer ovlivnilo chování občanů na veřejných prostranstvích. Navíc, vzhledem ke schopnostem a kapacitě těchto technologií, si zaměstnanci vůbec nemusí uvědomovat, jaké osobní údaje a pro jaké účely jsou zpracovávány a je dokonce možné, že ani nebudou o existenci sledovací technologie vědět.

Monitorování použití informačních technologií se také liší od jiných, viditelnějších sledovacích nástrojů, jako kamery, tím, že mohou fungovat skrytě. Pokud nebude k dispozici lehce pochopitelná a snadno dostupná politika sledování na pracovišti, nebudou zaměstnanci vědět o existenci a důsledcích tohoto monitorování a nebudou proto mít možnost výkonu svých práv. Další riziko spočívá v nadměrném shromažďování dat v takových systémech, které například sbírají lokační údaje z WiFi.

Nárůst objemu dat vytvářených v pracovním prostředí, v kombinaci s novými technikami analýzy a propojování, mohou také vytvářet rizika neslučitelná s dalším zpracováním. Příkladem takového nezákonného zpracování je použití systémů legitimně instalovaných k ochraně majetku pro sledování přítomnosti a výkonu zaměstnanců a jejich chování vůči zákazníkům. Jiným příkladem je použití dat shromážděných z kamer k pravidelnému sledování chování a výkonnosti zaměstnanců nebo využití údajů z geolokačního systému (např. sledování podle WiFi nebo Bluetooth) k nepřetržité kontrole pohybu a chování zaměstnance.

Takové sledování může zasahovat do zaměstnancova práva na soukromí bez ohledu na to, zda probíhá systematicky nebo příležitostně. Riziko neplyne jen z analýzy obsahu komunikace. Analýza metadat ve vztahu k určité osobě by také mohla představovat sledování života a vzorců chování jednotlivce, a tak být stejně dotěrná vůči jeho soukromí.

Rozsáhlé využití sledovacích technologií může rovněž snížit ochotu zaměstnanců (a omezit cesty, kterými by mohli) informovat zaměstnavatele o nepoctivém nebo nezákonném jednání nadřízených nebo jiných zaměstnanců ohrožující chod podnikání (zejména data zákazníků) nebo pracoviště. Aby se zaměstnanec odhodlal k takovému kroku a zmíněnou skutečnost oznámil, je často nezbytná jeho anonymita. Monitorování zasahující do zaměstnancových práv na soukromí může bránit nezbytné komunikaci s příslušnými pracovníky. V takovém případě se mohou zavedené prostředky pro interní oznamování (whistleblowing) stát neúčinnými[14].

5. Posouzení proporcionality

Tento oddíl rozebírá několik scénářů zpracování dat na pracovišti, kde nové technologie a/nebo rozvoj stávajících technologií má nebo může mít potenciálně za následek vysoké riziko pro soukromí zaměstnanců. Ve všech těchto případech by zaměstnavatelé měli zvážit zda:

- zpracovatelská činnost je nezbytná, a pokud ano, jaké právní důvody byly uplatněny;
- navrhované zpracování osobních údajů je z pohledu zaměstnanců korektní;
- zpracovatelská činnost je proporcionální vzhledem k vyjádřeným obavám; a
- zpracovatelská činnost je transparentní.

5.1 Zpracování během přijímacího řízení

Individuální využívání sociálních sítí je široce rozšířeno a je poměrně běžné, že profily uživatelů jsou veřejně viditelné, podle toho, jaké nastavení držitel účtu zvolil. Zaměstnavatelé tak mohou nabýt dojmu, že prohlížení profilů budoucích kandidátů na sociálních sítích je během náboru oprávněné. To samé může platit i pro jiné veřejně dostupné informace o možném zaměstnanci.

Zaměstnavatelé by se však neměli domnívat, že pouhá veřejná dostupnost osobního profilu na sociálních sítích jim dovoluje zpracovávat tato data pro své vlastní účely. Pro takové zpracování je potřeba mít právní důvod, jako třeba oprávněný zájem. Než začne prohlížet profil uchazeče na sociálních sítích, měl by zaměstnavatel zvážit, zda daný profil má obchodní nebo osobní účel, což může být důležitým ukazatelem zákonné přípustnosti prohlížení. Zaměstnavatelé navíc smí shromažďovat a zpracovávt osobní údaje vztahující se k žadateli o práci jen v rozsahu potřebném a podstatném z hlediska výkonu práce, o kterou je žádáno.

Údaje shromážděné během náboru by, obecně řečeno, měly být vymazány hned poté, co je jasné, že práce nebude dotyčnému jednotlivci nabídnuta nebo jím nebyla přijata[15]. Jednotlivce je také třeba náležitě informovat ještě před zahájením přijímacího řízení o každém zpracování.

Neexistuje žádný právní důvod pro to, aby zaměstnavatel požadoval po potenciálních zaměstnancích, aby ho zařadili mezi „přátele“nebo poskytli přístup k obsahu svých profilů jiným způsobem.

Příklad

[14] Viz například WP29, *Stanovisko 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, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_cs.pdf

[15] Vit také Rada Evropy, *Doporučení CM/Rec(2015)5 Výboru ministrů členským státům ohledně zpracování osobních údajů v souvislosti se zaměstnáním*, odstavec 13.2. (1. dubna 2015), url: https://search.coe.int/cm/Pages/result details.aspx?ObjectID=09000016805c3f7a). V případech, kdy zaměstnavatel chce data uchovat s výhledem na další pracovní nabídky, měl by být subjekt údajů příslušně informován a měl by dostat možnost vznést vůči dalšímu zpracování námitku, v kterémžto případě by data měla být vymazána (Id.).

Během náboru nových zaměstnanců kontroluje zaměstnavatel profily kandidátů na různých sociálních sítích a takto získané informace (a veškeré další informace dostupné na internetu) použije ve výběrovém řízení.

Zaměstnavatel může mít k prohlídce veřejně dostupných informací na sociálních sítích o kandidátech právní důvod podle článku 7 písm. f) jen, je-li to nezbytné například pro posouzení zvláštních rizik ve vztahu ke kandidátovi pro konkrétní funkci a tento byl náležitě informován (třeba v textu náborového inzerátu).

5.2 Zpracování při prověřování v průběhu zaměstnání

Díky existenci profilů na sociálních sítích a rozvoji nových analytických technologií jsou (nebo mohou být) zaměstnavatelé technicky schopni neustále prověřovat zaměstnance prostřednictvím sběru informací o jejich přátelích, názorech, přesvědčeních, zájmech, zvycích, majetku, postojích a chování a sbírat tak údaje, včetně citlivých, týkající se zaměstnancova soukromého a rodinného života.

Prověřování zaměstnaneckých profilů na sociálních sítích by se nemělo dít na obecném základě.

Zaměstnavatelé by navíc neměli po zaměstnanci nebo žadateli o práci požadovat přístup k informacím, které sdílí s ostatními prostřednictvím sociálních sítí.

Příklad
Zaměstnavatel monitoruje na LinkedIn profily bývalých zaměstnanců vázaných konkurenční doložkou. Účelem je ověřit dodržování této doložky. Sledování je omezeno pouze na tyto bývalé zaměstnance.

Pokud může 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 opřít o právní základ podle článku 7 písm. f) ve Směrnici o ochraně dat.

Po zaměstnancích by navíc nemělo být požadováno, aby používali zaměstnavatelem poskytnutý profil na sociálních médiích. Dokonce, i když je to specificky potřebné vzhledem k jejich úkolům (např. tiskový mluvčí), musí jim být ponechána možnost zvolit „nepracovní“ neveřejný profil, který budou moci používat místo „oficiálního“ služebního profilu a tato možnost by měla být v podmínkách pracovní smlouvy.

5.3 Zpracování při dohledu nad užíváním informačních a komunikačních technologií na pracovišti

Monitorování elektronické komunikace na pracovišti (např. telefon, surfování po internetu, e-mail, instant messaging, volání přes internet - VOIP, atd.) bylo tradičně považováno za hlavní hrozbu pro soukromí zaměstnanců. Ve svém *Pracovním dokumentu ke sledování elektronické komunikace na pracovišti* z roku 2001 došla WP29 k řadě závěrů ohledně sledování použití e-mailu a internetu. Tyto závěry sice zůstávají platné, je však potřeba vzít v potaz technologický rozvoj, který umožnil novější, potenciálně dotěrnější a všudypřítomné způsoby monitorování. Mezi tyto nové výdobytky, mimo jiné, patří:

- Nástroje prevence úniku dat (DLP), které sledují odchozí komunikaci za účelem odhalení možných úniků dat;
- Firewally nové generace a systémy zabezpečení sítě UTM, které mohou poskytovat řadu monitorovacích technologií včetně hloubkové inspekce paketů (DPI), kryptografický protokol TLS, filtrování webových stránek, filtrování obsahu, informace o totožnosti uživatele a (jak je popsáno výše) prevence úniku dat. Tyto technologie mohou také být nasazeny jednotlivě, podle rozhodnutí zaměstnavatele;

- Bezpečnostní aplikace a opatření zahrnující logovaný zaměstnanecký přístup do systémů zaměstnavatele;
- Technologie eDiscovery, která zahrnuje jakýkoliv proces vyhledávání elektronických dat pro jejich použití jako důkazu;
- Sledování využívání aplikací a zařízení přes neviditelný software, buď v osobním počítači nebo v cloudu;
- Použití na pracovišti kancelářských aplikací poskytovaných jako cloudová služba, které teoreticky umožňují velmi podrobné logování činnosti zaměstnanců;
- Monitorování vlastních osobních zařízení (např. PC, mobilní telefony, tablety), které zaměstnanci používají k práci v souladu s konkrétní uživatelskou politikou, jako je Přines si své vlastní zařízení (BYOD) nebo technologie Mobile Device Management (MDM) umožňující distribuci aplikací, dat a konfiguračních nastavení a záplat pro přenosná zařízení; a
- Použití nositelné elektroniky (např. zařízení pro sledování zdraví a fitness tréninku).

Je možné, že zaměstnavatel pro sledování zavede řešení „vše v jednom“, tedy sadu bezpečnostních balíčků, které dovolují sledovat veškeré nakládání s informačními technologiemi na pracovišti, na rozdíl od dříve používaného sledování e-mailu a/nebo webu. Závěry učiněné v dokumentu WP55 platí pro kterýkoliv systém umožňující takové sledování.[16]

Příklad

Zaměstnavatel hodlá nasadit zařízení TLS k dešifrování a kontrole zabezpečeného provozu za účelem odhalení čehokoliv nežádoucího. Toto zařízení dokáže zaznamenávat a analyzovat veškerou činnost zaměstnance v podnikové síti.

Roste počet použití šifrovaných komunikačních protokolů k ochraně online datových toků zahrnujících osobní údaje před jejich neoprávněným zachycením. To však může způsobovat problémy, protože šifrování znemožňuje sledovat příchozí a odchozí data. TLS dešifruje datový proud, analyzuje obsah z důvodu bezpečnosti a následně proud opět zašifruje.

V tomto případě se zaměstnavatel opírá o zákonné zájmy — potřebu chránit síť a v ní se nacházející osobní údaje zaměstnanců a zákazníků proti neoprávněnému vstupu nebo úniku. Avšak sledování veškeré činnosti zaměstnanců v online prostředí představuje nepřiměřené řešení a zásah do práva na důvěrnost komunikace. Zaměstnavatel by nejprve měl prozkoumat jiné, méně invazivní prostředky k ochraně důvěrnosti zákaznických dat a zabezpečení sítě.

Vzhledem k tomu, že určité zachycování provozu TLS může být kvalifikováno jako opravdu nezbytné, mělo by být zařízení konfigurováno způsobem předcházejícím neustálému logování zaměstnancovy činnosti, například blokováním podezřelého příchozího nebo odchozího provozu a přesměrováním uživatele na informační portál, kde může požádat o přezkum takového automatizovaného rozhodnutí. Bude-li nějaké obecné logování přece jen považováno za opravdu nezbytné, mělo by být zařízení nastaveno tak, aby nedocházelo k ukládání logů, pokud není signalizován výskyt nějakého incidentu, přičemž informace by měly být shromažďovány v minimálním rozsahu.

V rámci dobré praxe by zaměstnavatel mohl zaměstnancům nabídnout alternativní nemonitorovaný přístup. Lze to učinit poskytnutím volné WiFi nebo samostatných zařízení či terminálů (s náležitým zabezpečením důvěrnosti komunikace), kdy zaměstnanci mohou uplatnit své právo používat pracovní zařízení k některým soukromým potřebám[17]. Zaměstnavatelé by taky měli vzít v úvahu jisté druhy

[16] Viz také *Copland v United Kingdom*, (2007) 45 ESLH 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), ve kterém soud konstatoval, že e-maily odesílané z obchodních prostor a informace získané z monitorování používání internetu by mohly být součástí soukromého života zaměstnance a jeho korespondence, a že sběr a uchovávání takových informací bez vědomí dotyčného zaměstnance by představovalo zásah do jeho práv, ačkoliv soud nerozhodl, že takové sledování by nikdy nebylo v demokratické společnosti potřebné.

[17] Viz *Halford v. Spojené království*, [1997] ESLH 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html'). Soud konstatoval, že „v souvislosti s telefonními hovory z obchodních prostor stejně jako z domova lze uplatnit pojem ‚soukromý život' a ‚korespondence' ve významu podle článku 8 odst. 1 [Úmluvy]“; a *Barbulescu v.*

provozu, kde zachycování ohrožuje řádnou rovnováhu mezi jejich oprávněnými zájmy a soukromím zaměstnance — jako třeba používání soukromého webmailu, internetového bankovnictví a návštěvy zdravotnických webových stránek — v zájmu patřičné konfigurace zařízení, aby nezasahovalo do komunikace za podmínek, jež nejsou v souladu se zásadou proporcionality. Informace o druzích komunikace, které zařízení sleduje, by měla být zaměstnancům k dispozici.

Měla by být vypracována politika k otázce účelů, tedy kdo a kdy bude mít přístup k přihlašovacím údajům (logům) a tento dokument by měl být snadno dostupný všem zaměstnancům, také jako vodítko ohledně přípustného a nepřípustného využívání sítě a zařízení. Zaměstnanci tak budou moci přizpůsobit své chování ve snaze předejít sledování během legitimního použití informačních technologií a zařízení pro soukromé potřeby. Je osvědčeným postupem takovou politiku alespoň jednou ročně vyhodnotit a posoudit, zda zvolené řešení monitoringu přineslo očekávané výsledky a zda k danému účelu neexistují méně narušující nástroje nebo prostředky.

Bez ohledu na danou technologii nebo její schopnosti je právní důvod podle článku 7 písm. f) uplatnitelný, jen pokud zpracování splňuje určité podmínky. Zaměstnavatelé, kteří používají tyto produkty a aplikace, musí především zvážit proporcionalitu zaváděných opatření a zda není potřeba učinit další kroky ke zmírnění nebo omezení rozsahu a dopadu daného zpracování dat. Jako příklad dobré praxe lze zmínit, že toto lze učinit cestou posouzení vlivu před nasazením sledovací technologie. Zaměstnavatelé musí dále zavést a ohlásit přijatelnou uživatelskou politiku spolu se zásadami ochrany soukromí, kde vysvětlí dovolené používání firemní sítě a vybavení, přičemž podrobně uvedou, jaká zpracování probíhají.

V některých zemích bude takto vypracovaná politika vyžadovat souhlas podnikové rady nebo podobného orgánu zastupujícího zaměstnance. V praxi tyto politiky často navrhují zaměstnanci IT oddělení. Ti se převážně soustřeďují na bezpečnost a nikoliv na oprávněná očekávání zaměstnanců ohledně ochrany jejich soukromí, proto WP29 doporučuje, aby do posuzování potřebnosti monitoringu i znění a dostupnosti příslušné politiky byla vždy zapojena reprezentativní skupina zaměstnanců .

Příklad

Zaměstnavatel instaluje systém prevence úniku dat (DLP) k automatickému sledování odchozích e-mailů jako prevenci neoprávněného přenosu dat, na něž se vztahují vlastnická práva (např. osobní údaje zákazníků), bez ohledu, zda je taková akce neúmyslná či nikoliv. Jakmile je nějaký e-mail pokládán za možný zdroj úniku dat, provede se další šetření.

I v tomto případě je zákonným zájmem zaměstnavatele chránit osobní údaje zákazníků i svůj majetek před neoprávněným přístupem nebo datovým únikem. Přesto může tento nástroj (DLP) s sebou nést nepotřebné zpracování osobních údajů — například „falešný“ poplach by mohl vést k neoprávněnému přístupu k legitimním e-mailům odeslaným zaměstnanci (což mohou být i osobní e-maily).

Proto by nezbytnost nástroje DLP a jeho zavedení měla být plně odůvodněna v zájmu dosažení náležité rovnováhy mezi legitimními zájmy a základním právem na ochranu osobních údajů zaměstnanců. Aby se zaměstnavatel mohl opřít o zákonné zájmy, měl by uplatnit určitá opatření ke zmírnění rizik. Například by uživatelům mělo být zcela jasné, podle jakých pravidel systém klasifikuje e-mail jako možné porušení bezpečnosti dat a v případě, že e-mail, který má být odeslán, je rozpoznán jako možný

Rumunsko, [2016] ESLH 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), ohledně použití služebního účtu instant messenger k osobní korespondenci, kde soud řekl, že monitorování účtu zaměstnavatelem bylo omezené a proporcionální; v oponujícím stanovisku soudce Pinto de Alberquerque argumentoval potřebou dosažení pečlivé rovnováhy.

únik dat, měl by o tom systém odesílatele varovnou zprávou informovat ještě před odesláním, aby měl možnost přenos zrušit.

V některých případech je sledování zaměstnanců umožněno ne tak v důsledku instalace specifických technologií, ale prostě proto, že se od zaměstnanců očekává, že budou používat aplikace poskytnuté zaměstnavatelem, a které zpracovávají osobní údaje. Využívání kancelářských aplikací v cloudu (např. textové editory, kalendáře, sociální sítě) je takovým příkladem. Zaměstnancům by mělo být umožněno, aby si mohli vytvořit určitá soukromá místa, kam se zaměstnavatel nedostane, pokud nenastanou výjimečné okolnosti. To je například důležité v případě kalendářů často používaných i pro záznam soukromých termínů. Pokud zaměstnanec nějakou schůzku označí jako „soukromou“ nebo to uvede v záznamu samotném, pak by zaměstnavatelům (a ani jiným zaměstnancům) nemělo být dovoleno do obsahu takového záznamu nahlédnout.

Požadavek subsidiarity může někdy v této souvislosti znamenat, že k monitorování nesmí docházet vůbec. Příkladem je situace, kdy zakázanému používání komunikačních služeb může být zabráněno blokováním určitých webových stránek. Je-li možné webové stránky blokovat namísto neustálého sledování veškeré komunikace, mělo by být blokování zvoleno v souladu s požadavkem subsidiarity.

Obecně by prevence měla mít přednost před detekcí — zájmy zaměstnavatele lze lépe ochránit předcházením zneužití internetu pomocí technických nástrojů, než vynakládáním zdrojů na jeho zjišťování.

5.4 Zpracování při monitorování využití informačních a komunikačních technologií mimo pracoviště

Použití informačních a komunikačních technologií mimo pracoviště se stává běžným v důsledku rostoucího počtu případů práce z domova, na dálku a politiky „přines si svůj vlastní přístroj“. Možnosti těchto technologií mohou ohrožovat soukromý život zaměstnanců, protože mnohdy jsou sledovací systémy existující na pracovišti účinně nasazovány i do domácí sféry zaměstnanců, když příslušné zařízení používají.

5.4.1 *MONITOROVÁNÍ DOMOVA A PRÁCE NA DÁLKU*

Zaměstnavatelé častěji nabízí zaměstnancům možnost práce na dálku např. z domova a/nebo během přepravy. Tato skutečnost vede k omezenému rozlišování mezi pracovištěm a domovem. To se v obecné rovině dotýká zaměstnavatele, který zaměstnancům poskytuje prostředky informační a komunikační techniky nebo software, který, pokud je nainstalován u nich doma nebo na jejich vlastních zařízeních, jim umožňuje stejnou úroveň přístupu do zaměstnavatelovy sítě, k systémům a zdrojům, který by, v závislosti na provedení, měli, i pokud by byli na pracovišti.

Práce na dálku může být vnímána pozitivně, představuje však pro zaměstnavatele další oblast rizika. Zaměstnanci, kteří mají vzdálený přístup k zaměstnavatelově infrastruktuře například nejsou vázáni fyzickými bezpečnostními opatřeními, které mohou být k dispozici v prostorách pracoviště. Řečeno jasně: bez zavedení náležitých technických opatření roste riziko neoprávněného přístupu, které může vyústit až ve ztrátu nebo zničení informací, včetně osobních údajů zaměstnanců nebo zákazníků, jež jsou v držení zaměstnavatele.

Za účelem zmírnění tohoto rizika mohou zaměstnavatelé přijít na myšlenku, že je odůvodnitelné instalovat (přímo v místě práce nebo v cloudu) software, který umí, například, logovat údery kláves a pohyby myší, ukládat otisk obrazovky (náhodně nebo v zadaných intervalech), logovat užití aplikací (a jak dlouho a k čemu byly použity) a – na kompatibilních přístrojích – umožňuje provoz webové kamery a sběr záznamů z této kamery. Takové technologie jsou široce dostupné také od třetích stran, jako jsou poskytovatelé cloudu.

Zpracování, které s sebou tyto technologie nese, je však nepřiměřené a je velmi nepravděpodobné, že by tu byl právní důvod založený na oprávněném zájmu zaměstnavatele, např. k záznamu úderů kláves a pohybů myší, které zaměstnanec provedl.

Je zásadní, aby riziko v důsledku práce z domova nebo na dálku bylo ošetřeno proporcionálně, nepřehnaně, ať už je výběr nabídnut jakýmkoliv způsobem a za použití jakékoliv technologie, zvláště pokud jsou hranice mezi služebním a soukromým používáním nejisté.

5.4.2 *PŘINES SI SVÉ VLASTNÍ ZAŘÍZENÍ (BYOD)*

Vzhledem k nárustu oblíbenosti, funkcionality a schopností přístrojů spotřební elektroniky se zaměstnavatelé mohou setkávat s požadavky zaměstnanců, aby mohli k výkonu práce na pracovišti používat své vlastní přístroje. Uchytil se název „bring your own device“ zkráceně BYOD.

BYOD skutečně může zaměstnancům přinášet četné výhody, včetně většího uspokojení z práce, povšechného zvýšení morálky, větší efektivity a flexibility. Z podstaty věci však vyplývá, že zařízení zaměstnance bude používáno i pro osobní potřebu, pravděpodobně především v určitých fázích dne (např. po večerech nebo o víkendech). Nesporně tedy používání vlastních přístrojů zaměstnanci povede k tomu, že zaměstnavatelé budou zpracovávat nefiremní informace o dotčených zaměstnancích a případně také o jejich rodinných příslušnících, kteří mohou tyto přístroje také používat.

V kontextu zaměstnávání souvisí obvykle rizika BYOD pro soukromí se sledovacími technologiemi, které shromažďují identifikátory, jako jsou MAC adresy nebo s případy, kdy zaměstnavatel vstupuje do zařízení zaměstnance kvůli bezpečnostní kontrole, tj. odhalování škodlivého softwaru. Pro tento druhý případ existuje mnoho komerčních řešení, která dovolují prohlížet soukromá zařízení, jejich použití však může umožnit přístup ke všem datům v tomto zařízení a proto je potřeba s nimi zacházet opatrně. Například, do těch částí zařízení, o kterých se předpokládá, že jsou používány jen pro soukromé účely (např. složka s fotografiemi pořízenými tímto zařízením) by v zásadě nemělo být vstupováno.

Sledování polohy a provozu těchto zařízení lze brát jako činnost sloužící oprávněným zájmům chránit osobní údaje, za které zaměstnavatel coby správce nese odpovědnost; může to však být nezákonné, jde-li o soukromý přístroj zaměstnavatele a sledováním jsou shromažďována i data týkající se soukromého a rodinného života zaměstnance. Aby se předešlo sledování soukromých informací, je třeba zavést příslušná opatření k rozlišení mezi soukromým a služebním použitím přístroje.

Zaměstnavatelé by také měli uplatnit metody bezpečného přenosu svých vlastních dat mezi soukromými zařízeními a podnikovou sítí. Zařízení může třeba být konfigurováno tak, aby veškerou komunikaci směrovalo přes VPN do podnikové sítě, čímž by byla zajištěna jistá úroveň zabezpečení; je-li však takové opatření použito, měl by si zaměstnavatel uvědomit, že software nainstalovaný pro účely sledování s sebou nese riziko pro soukromí během doby, kdy zaměstnanec zařízení používá soukromě. Mohlo by být využito zařízení, které nabízí dodatečnou ochranu jako je technika „sandboxing“ (uchovávání dat odděleně v určité konkrétní aplikaci).

Naopak, zaměstnavatel musí také zvážit uplatnění zákazu používat konkrétní pracovní zařízení pro soukromé účely, neexistuje-li způsob, jak takovému použití předejít monitorováním — například pokud zařízení umožňuje vzdálený přístup k osobním údajům, vůči nimž je zaměstnavatel správcem.

5.4.3 *SPRÁVA MOBILNÍCH ZAŘÍZENÍ (MDM)*

Správa mobilních zařízení umožňuje zaměstnavatelům na dálku zjistit polohu zařízení, provádět specifické konfigurace a/nebo instalovat aplikace či mazat „data on demand“. Zaměstnavatel může tuto funkcionalitu provozovat sám nebo k tomu využít třetí stranu. Služby MDM zaměstnavatelům také umožňují sledovat zařízení nebo z něj ukládat informace v reálném čase, dokonce i když není nahlášeno jako ukradené.

Posouzení vlivu na ochranu osobních údajů by mělo být vypracováno před nasazením jakékoliv takové technologie, pokud je nová jako taková nebo nová pro správce. Ukáže-li toto posouzení, že technologie

MDM je ve specifických podmínkách nezbytná, mělo by přesto být posouzeno, zda související zpracování dat bude v souladu se zásadou proporcionality a subsidiarity. Zaměstnavatelé musí zajistit, aby data získaná při zjišťování polohy na dálku byla zpracována pro stanovený účel a a nebyla či nemohla být součástí rozsáhlejšího programu umožňujícího průběžné sledování zaměstnanců. Sledovací funkce by měly být redukovány i v případě nasazení pro konkrétní účely. Sledovací systémy mohou být navrženy tak, aby zaznamenávaly údaje o poloze, aniž by pak byla poskytnuta zaměstnavateli — v takovém případě by lokalizační údaje měly být dostupné jen, pokud by došlo ke ztrátě zařízení.

Zaměstnanci, na jejichž zařízení jsou aplikovány služby MDM, musí být také plně informováni o tom, jaké sledování probíhá a jaké důsledky pro ně může mít.

5.4.4 *NOSITELNÁ ZAŘÍZENÍ*

Zaměstnavatelé jsou stále více v pokušení vybavit své zaměstnance nositelnými zařízeními, aby mohli sledovat a kontrolovat jejich zdraví a činnost na pracovišti a někdy i mimo něj. Takové zpracování dat však zahrnuje i zdravotní údaje a je tedy podle článku 8 Směrnice o ochraně dat zakázáno.

Vzhledem k nerovnému vztahu mezi zaměstnavateli a zaměstnanci — zaměstnanec je například na zaměstnavateli finančně závislý — a citlivé povaze zdravotních dat, je vysoce nepravděpodobné, že by pro sledování a kontrolu takových dat mohl být udělen podle zákona platný výslovný souhlas, neboť zaměstnanci v zásadě nemají svobodu takový souhlas dát. Zpracování bude nezákonné dokonce i tehdy, pokud zaměstnavatel využije ke sběru zdravotních dat třetí stranu, která mu dodá jen agregované informace o obecné zdravotní situaci.

Jak je také popsáno ve Stanovisku *5/2014 k technikám anonymizace*[18], je technicky velmi obtížné zajistit úplnou anonymizaci dat. Dokonce i v prostředí s více než tisíci zaměstnanci by zaměstnavatel dokázal, vzhledem k dostupnosti dalších dat o zaměstnancích, vyčlenit konkrétního pracovníka se zvláštními zdravotními parametry, například s vysokým krevním tlakem nebo s obezitou.

Příklad:

Organizace nabídne zaměstnancům jako dárek sledovací zařízení pro fitness. Tento přístroj počítá kroky a zaznamenává tep a spací návyky zaměstnanců.

Takto získaná zdravotní data by měla být dostupná jen zaměstnanci a ne zaměstnavateli. Jakékoliv údaje přenesené mezi zaměstnancem (subjekt údajů) a poskytovatelem zařízení/služby (správce) jsou záležitostí těchto stran.

Jelikož by zdravotní data mohla být zpracovávána i výrobcem zařízení nebo poskytovatelem služby, měl by zaměstnavatel při výběru zařízení nebo služby vyhodnotit politiku ochrany soukromí výrobce nebo poskytovatele, aby měl jistotu, že nedojde k nezákonnému zpracování zdravotních údajů zaměstnanců.

5.5 Zpracování týkající se pracovní doby a docházky

Systémy umožňující zaměstnavatelům kontrolovat, kdo vstupuje, resp. může vstoupit, do jejich prostor a/nebo do jejich určitých částí, mohou umožňovat také sledování činnosti zaměstnanců. Ačkoliv tyto systémy existují již řadu let, jsou nové technologie ke sledování pracovní doby a docházky využívány mnohem více, včetně takových, které zpracovávají biometrická data nebo prostředků ke sledování mobilních zařízení.

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

Tyto systémy mohou být důležitou součástí auditu zaměstnavatele, přinášejí však také riziko získávání invazivního rozsahu povědomí o činnostech zaměstnance na pracovišti a jejich kontroly.

Příklad:
Zaměstnavatel provozuje serverovnu, kde jsou v digitální podobě ukládána podnikově citlivá data a osobní údaje zaměstnanců i zákazníků. Z důvodu dodržení zákonných povinností ohledně zabezpečení dat proti neoprávněnému přístupu nainstaloval zaměstnavatel systém kontroly vstupu, který zaznamenává příchod a odchod zaměstnanců s náležitým vstupním oprávněním. Pokud by došlo ke ztrátě části vybavení nebo k neoprávněnému přístupu k datům, jejich ztrátě nebo krádeži, pak zaměstnavatel na podkladě uchovávaných záznamů dokáže zjistit, kdo v dané době do místnosti vstoupil.

Vzhledem k tomu, že zpracování je nutné a nepřevažuje nad právem na soukromý život zaměstnanců, může tedy být podle článku 7 písm. f) v oprávněném zájmu, pokud byli zaměstnanci o operaci zpracování náležitě informováni. Stálé monitorování četnosti a času vstupu a odchodu zaměstnanců bude neodůvodnitelné, pokud budou takto získané údaje použity i pro jiný účel, například hodnocení výkonu zaměstnance.

5.6 Zpracování s použitím systémů kamerového sledování

Kamerové sledování a dohled nadále představuje téma z hlediska soukromí zaměstnanců: schopnost průběžně zachycovat chování pracovníka.[19] Nejpodstatnější změny týkající se aplikace této technologie v souvislosti se zaměstnáním souvisí s možností snadno přistupovat ke shromážděným údajům dálkově (např. přes chytrý telefon), dále se zmenšením velikosti kamer (souběžně s nárůstem schopností, např. vysoké rozlišení) a s ohledem na fakt, že zpracování může být nově prováděno prostřednictvím videoanalýzy.

Pomocí videoanalýzy může zaměstnavatel automatizovaně sledovat výraz obličeje pracovníka, rozpoznat odchylky od přednastavených pohybových vzorců (např. v továrnách) a mnoho dalšího. To by bylo neproporcionální ve vztahu k právům a svobodám zaměstnanců a obecně proto nezákonné. Je pravděpodobné, že zpracování bude zahrnovat profilování, popřípadě i automatizované rozhodování. Zaměstnavatelé by proto měli upustit od použití technologií na rozpoznávání obličeje. Mohou se vyskytnout určité okrajové výjimky, ale těmito scénáři nelze obecně legitimizovat použití takové technologie[20].

5.7 Zpracování zahrnující vozy používané zaměstnanci

Technologie umožňující zaměstnavatelům sledovat svá auta je široce uplatňována, hlavně u organizací, které se zabývají dopravou nebo mají velké flotily služebních vozů.

Zaměstnavatel, který používá ve vozech telematiku, shromažďuje data jak o vozidle, tak o zaměstnanci, jenž auto používá. Tato data mohou zahrnovat nejenom informace o poloze vozidla (a tím také zaměstnance) získaná pomocí jednoduchého sledovacího systému na bázi GPS, ale, podle té které technologie, spoustu dalších informací včetně řidičova chování. Určité technologie také umožňují nepřetržité sledování vozidla i řidiče (např. zapisovač událostí).

Zaměstnavatel by mohl být povinen instalovat sledovací techniku do vozidel, aby prokázal soulad s dalšími právními povinnostmi, např. pro zajištění bezpečnosti zaměstnanců, kteří je řídí. Zaměstnavatel může mít rovněž oprávněný zájem na tom, aby mohl kdykoliv zjistit polohu vozidel. I kdyby zaměstnavatelé měli oprávněný zájem k dosažení těchto účelů, měli by nejprve posoudit, zda je zpracování pro tyto účely nezbytné a zda zavedení těchto opatření bude v souladu se zásadami

[19] Viz výše zmíněný případ *Köpke v. Německo;* dodatečně lze uvést, že v některých jurisdikcích byla instalace systémů typu kamerového dohledu za účelem prokázání nezákonného jednání shledána přípustnou; viz případ *Bershka* u Ústavního soudu ve Španělsku.

[20] Podle Obecného nařízení navíc musí být zpracování biometrických údajů pro účely identifikace založeno na výjimce podle článku 9 odst. 2.

proporcionality a subsidiarity. Je-li dovoleno soukromé použití služebního vozu, bude nejdůležitějším opatřením, které zaměstnavatel může učinit pro dodržení těchto principů, nabídnutí „odstupní“ možnosti (opt-out): zaměstnanec by v zásadě měl mít možnost dočasně vypnout sledování polohy vždy, kdy k tomu zvláštní okolnosti opravňují, třeba při návštěvě lékaře. Tímto způsobem může zaměstnanec z vlastní iniciativy ochraňovat určitá data o poloze jako soukromá. Zaměstnavatel musí zajistit, aby shromažďovaná data nebyla použita k nezákonnému dalšímu zpracování, jaké představují sledování a vyhodnocování zaměstnanců.

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 v každém voze.

Zaměstnanci někdy mohou služební auta používat i mimo pracovní dobu, pro osobní účely, podle toho, jak určuje konkrétní firemní politika. Vzhledem k citlivosti údajů o poloze je málo pravděpodobné, že by existoval právní důvod k monitorování polohy služebních aut řízených zaměstnancem mimo pracovní hodiny. Pokud by to však nutné bylo, je třeba vzít v úvahu proporcionalitu, která by byla přiměřená rizikům. Například by to mohlo znamenat, že kvůli prevenci krádeže auta, nebude jeho poloha mimo pracovní dobu zaznamenávána, dokud vůz neopustí široce definovaný územní okruh (oblast nebo dokonce zemi). Kromě toho by poloha měla být zobrazována jen způsobem, kdy zaměstnavatel aktivuje „viditelnost“ polohy přistoupením k systémem již uloženým datům, když vozidlo opustí předem definovanou oblast.

V dokumentu WP29 *Stanovisko 13/2011 ke geolokalizačním službám u inteligentních mobilních zařízení* se říká[21]:

> „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.“

A dále, jak WP29 uvedla ve *Stanovisku 5/2005 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou*[22]*:*

> „Zpracování lokalizačních údajů může být odůvodněné v případech, kdy slouží k 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 ZAPISOVAČE UDÁLOSTÍ

Zapisovače událostí zaměstnavateli technicky umožňují zpracovávat značné množství osobních údajů o zaměstnancích, kteří řídí služební vozy. Tato zařízení jsou stále častěji umísťována do aut za účelem obrazového, a pokud možno i zvukového záznamu případné nehody. Tyto systémy dokážou začít nahrávat v určitém okamžiku, např. při náhlém brzdění, náhlé změně směru nebo nehodě, přičemž

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

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

zaznamenají a uloží okamžiky bezprostředně před incidentem, ovšem mohou také být v provozu a monitorovat nepřetržitě. Takto získané informace mohou být později použity k pozorování a kontrole řidičova chování za účelem jeho vylepšení. Mnoho těchto systémů navíc obsahuje GPS pro sledování polohy vozidla v reálném čase a dalších podrobností souvisejících s řízením (rychlost jízdy), které lze uchovávat pro další zpracování.

Nasazení těchto zařízení převažuje u organizací zabývajících se přepravou nebo mají velké flotily služebních vozů. Použití zapisovačů událostí však může být zákonné jen tehdy, existuje-li nezbytnost zpracovávat takto získané osobní údaje o zaměstnancích pro legitimní účel, a pokud toto zpracování bude v souladu se zásadami proporcionality a subsidiarity.

Příklad

Dopravní společnost vybavuje kabinu všech vozidel videokamerou zaznamenávající zvuk i obraz. Účelem zpracování takto získaných dat je vylepšování řidičských dovedností zaměstnanců. Kamery jsou konfigurovány tak, aby uchovaly záznam vždy, kdy dojde k náhlému brzdění nebo změně směru. Firma se domnívá, že má právní důvod ke zpracování podle článku 7 písm. f) Směrnice o ochraně dat, kterým je ochrana bezpečnosti vlastních zaměstnanců i ostatních řidičů.

Avšak zákonný zájem společnosti monitorovat řidiče nepřevažuje nad právy těchto řidičů na ochranu jejich osobních údajů. Ustavičné sledování zaměstnanců prostřednictvím kamer představuje závažný zásah do jejich práva na soukromí. Existují jiné způsoby (např. instalace zařízení zabraňujícího použít mobilní telefon) ,jakož i další bezpečnostní zařízení, jako pokročilý nouzový brzdný systém nebo systém varování před opuštěním jízdního pruhu, které mohou být pro prevenci autonehody mnohem vhodnější. Video navíc s vysokou pravděpodobností povede ke zpracování osobních údajů třetích stran (chodci) a pro takové zpracování nebude zákonný zájem firmy dostatečně odůvodnitelný.

5.8 Zpracování zahrnující zpřístupnění zaměstnaneckých dat třetím stranám

Stalo se běžným, že firmy zasílají zákazníkům údaje svých zaměstnanců, aby zajistily poskytnutí spolehlivé služby. Rozsah těchto dat může být docela značný, podle palety poskytovaných služeb (např. může být přiloženo foto zaměstnance). Zaměstnanci však nejsou v postavení, vzhledem k nerovnováze sil, kdy by mohli dát zaměstnavateli svobodný souhlas se zpracováním svých osobních údajů, a pokud by zpracování nebylo proporcionální, neměl by zaměstnavatel právní důvod.

Příklad:

Zásilková firma pošle svým zákazníkům e-mail s odkazem na jméno a polohu doručitele (zaměstnance). Firma také hodlá poskytnout jeho fotografii v pasové velikosti. Společnost předpokládá, že má pro zpracování právní důvod vzhledem k oprávněnému zájmu (Článek 7 písm. f) Směrnice o ochraně dat), kdy si zákazník může ověřit, zda doručitel je opravdu ta správná osoba.

Poskytovat zákazníkům jméno a fotografii doručitele však není nutné. Jelikož pro takové zpracování neexistuje žádný jiný právní důvod, nesmí zásilková společnost poskytovat tyto osobní údaje zákazníkům.

5.9 Zpracování zahrnující mezinárodní předávání personalistických a jiných údajů o zaměstnancích

Zaměstnavatelé stále více používají cloudové aplikace a služby, třeba pro správu personalistických dat nebo online kancelářských aplikací. Použití většiny těchto aplikací bude mít za následek mezinárodní předávání dat od zaměstnanců a o zaměstnancích. Jak už bylo dříve vysvětleno ve Stanovisku 08/2001, článek 25 Směrnice o ochraně dat stanoví, že přenosy osobních údajů do třetí země mimo EU mohou být uskutečněny, jen pokud daná země poskytuje odpovídající úroveň ochrany dat. Ať už základ bude jakýkoliv, předání by mělo vyhovovat ustanovením Směrnice o ochraně dat.

Měl by být tedy zajištěn soulad s ustanoveními ohledně mezinárodního předávání dat. WP29 znovu potvrzuje svůj dřívější názor, že je lepší spolehnout se na faktor odpovídající ochrany, než na výjimky vyjmenované v článku 26 Směrnice o ochraně dat; pokud je předání opřeno o souhlas, musí tento být určitý, jednoznačný a svobodný. Mělo by však rovněž být zajištěno, že rozsah dat sdílených mimo EU/EHP, jakož i následný přístup k nim ze strany dalších subjektů v rámci skupiny, zůstane omezen na nezbytné minimum potřebné k zamýšlenému účelu.

6. Závěry a doporučení

6.1 Základní práva

Na obsah komunikace výše uvedeného typu i na provozní údaje týkající se této komunikace se vztahují stejná základní práva jako na komunikaci „analogovou“.

Na elektronickou komunikaci činěnou z obchodních prostor se mohou vztahovat pojmy „soukromý život“ a „korespondence“ ve smyslu článku 8 odst. 1 Evropské úmluvy. Podle nynější Směrnice o ochraně dat 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.

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. Sledování polohy zaměstnanců přes jejich vlastní nebo firemní zařízení by mělo být omezeno na míru nezbytně nutnou k naplnění oprávněného účelu. V případě soukromě vlastněného přístroje používaného k práci (BYOD) je nutné, aby zaměstnanci dostali možnost odstínit soukromou komunikaci od jakéhokoliv s prací souvisejícího sledování.

6.2 Souhlas; oprávněný zájem

Zaměstnanci nejsou téměř nikdy v postavení, aby mohli dát souhlas svobodně nebo ho odmítnout či odvolat, což je dáno závislostí vyplývající ze vztahu zaměstnavatel/zaměstnanec. Vzhledem k nerovnováze sil mohou zaměstnanci udělit svobodný souhlas jen za výjimečných okolností, kdy souhlas nebo odmítnutí nevyvolá žádné následky.

Oprávněný zájem zaměstnavatelů může být někdy uplatněn jako zákonný důvod, avšak jen pokud zpracování je skutečně nutné pro tento oprávněný zájem a splňuje zásady proporcionality a subsidiarity. Test proporcionality by měl být proveden před nasazením jakéhokoliv monitorovacího nástroje, aby se zvážilo, 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.

6.3 Transparentnost

Zaměstnanci by měli být účinným způsobem informováni o jakémkoliv na pracovišti probíhajícím sledování, jeho účelech a okolnostech, jakož i o možnostech, jak mohou předcházet záznamu svých dat sledovacími technologiemi. Politiky a pravidla ohledně zákonného sledování musí být jasné a snadno dostupné. Pracovní skupina WP29 doporučuje zapojit reprezentativní skupinu zaměstnanců do tvorby a hodnocení takových pravidel a politik, jelikož monitorování má většinou potenciál zasahovat do soukromého života zaměstnanců.

6.4 Proporcionalita a minimalizace údajů

Zpracování dat na pracovišti musí být proporcionální odpovědí na rizika, kterým zaměstnavatel čelí. Například zneužívání internetu lze odhalit bez nutnosti analyzovat obsah webové stránky. Jde-li zneužití předejít (např. použitím webových filtrů), nemá zaměstnavatel na monitorování žádné obecné právo.

Plošný zákaz komunikace pro osobní účely je nepraktický a jeho prosazování by mohlo vyžadovat neproporcionální míru sledování. Větší důraz by měl být kladen na prevenci, než na odhalování – zájmům zaměstnavatele poslouží lépe prevence zneužití internetu prostřednictvím technických prostředků, než vynakládání zdrojů na jeho odhalování.

Informace zaznamenávané cestou nepřetržitého sledování, stejně jako informace, které jsou zaměstnavateli předkládány, by měly být co možná nejvíce minimalizovány. Zaměstnanci by měli mít možnost, za důvodných okolností, dočasně vypnout sledování polohy. Systémy, které sledují například polohu vozidel, mohou být řešeny tak, aby údaje o poloze registrovaly, aniž by je dále poskytovaly zaměstnavateli.

Zaměstnavatelé musí při rozhodování o nasazení nových technologií brát v úvahu minimalizaci údajů. Informace by měly být uchovány jen po skutečně nezbytnou, konkrétně stanovenou dobu. Vždy, kdy už informace není potřeba, měla by být smazána.

6.5 Cloudové služby, online aplikace a mezinárodní předávání

Pokud se od zaměstnanců očekává použití online aplikací zpracovávajících osobní údaje (jako třeba kancelářské online aplikace), měli by zaměstnavatelé zvážit, zda zaměstnancům nevymezit určité soukromé prostory, kam by zaměstnavatel nemohl za žádných okolností získat přístup, např. soukromý e-mail nebo složka dokumentů.

Použití většiny aplikací v cloudu bude znamenat mezinárodní předání zaměstnaneckých údajů. Mělo by být zajištěno, že předání osobních údajů do třetí země mimo EU se uskuteční, jen pokud bude zajištěna odpovídající úroveň ochrany, a že rozsah dat sdílených mimo EU/EHP a další přístup k nim jinými subjekty v rámci skupiny zůstane omezen na nezbytné minimum pro naplnění zamýšlených účelů.

* * *

V Bruselu, dne 8. června 2017

Za Pracovní skupinu,
předsedkyně
Isabelle FALQUE-PIERROTIN