PRACOVNÁ SKUPINA PRE OCHRANU ÚDAJOV ZRIADENÁ PODĽA ČLÁNKU 29

17/SK

WP 249

Stanovisko č. 2/2017 k spracúvaniu údajov v práci

Prijaté 8. júna 2017

Obsah

1 Zhrnutie

Toto stanovisko dopĺňa predchádzajúce publikácie pracovnej skupiny zriadenej podľa článku 29, konkrétne *Stanovisko č. 8/2001 k spracúvaniu osobných údajov v súvislosti s pracovným pomerom* (WP 48)[1] a *Pracovný dokument o dohľade nad elektronickými komunikáciami na pracovisku* (WP 55)[2]. Od uverejnenia týchto dokumentov bolo prijatých niekoľko nových technológií, ktoré umožňujú systematickejšie spracúvanie osobných údajov zamestnancov v práci, čím vznikajú značné problémy pre ochranu súkromia a osobných údajov.

V tomto stanovisku sa znovu posudzuje rovnováha medzi oprávnenými záujmami zamestnávateľov a odôvodnenými očakávaniami zamestnancov v oblasti ochrany súkromia, a to tak, že sa v ňom opisujú riziká, ktoré prinášajú nové technológie, a uskutočňuje posúdenie proporcionality niekoľkých scenárov, v ktorých by sa tieto technológie mohli použiť.

Hoci sa stanovisko zaoberá predovšetkým smernicou o ochrane údajov, zohľadňuje dodatočné povinnosti, ktoré zamestnávateľom vyplývajú zo všeobecného nariadenia o ochrane údajov. Opakuje sa v ňom postoj a závery zo stanoviska č. 8/2001 a pracovného dokumentu WP 55, konkrétne to, že pri spracúvaní osobných údajov zamestnancov:

- by zamestnávatelia vždy mali pamätať na základné zásady ochrany osobných údajov bez ohľadu na použitú technológiu,
- sa na obsah elektronickej komunikácie, ktorá sa uskutočnila z prevádzkových priestorov, vzťahuje rovnaká ochrana základných práv ako na analógovú komunikáciu,
- je veľmi nepravdepodobné, že právnym základom na spracúvanie údajov v práci bude súhlas, pokiaľ zamestnanci nemôžu odmietnuť spracúvanie bez nepriaznivých následkov,
- sa možno niekedy odvolať na plnenie zmluvy a oprávnené záujmy, a to za predpokladu, že spracúvanie je jednoznačne nevyhnutné na legitímny účel a že je v súlade so zásadami proporcionality a subsidiarity,
- zamestnanci by mali dostať účelné informácie o prebiehajúcom monitorovaní a
- každý medzinárodný prenos údajov zamestnancov by sa mal uskutočniť iba vtedy, keď je zabezpečená primeraná úroveň ochrany.

2. Úvod

Rýchle prijatie nových informačných technológií na pracovisku, pokiaľ ide o infraštruktúru, aplikácie a inteligentné zariadenia, umožňuje nové typy systematického a potenciálne invazívneho spracúvania údajov v práci. Napríklad:

[1] Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 8/2001 k spracúvaniu osobných údajov v súvislosti s pracovným pomerom*, WP 48, 13. septembra 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf.

[2] Pracovná skupina zriadená podľa článku 29, *Pracovný dokument o dohľade nad elektronickými komunikáciami na pracovisku*, WP 55, 29. mája 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf.

- technológie, ktoré umožňujú spracúvanie osobných údajov v práci, sa teraz môžu zaviesť za zlomok ceny spred niekoľkých rokov, kým kapacita spracúvania osobných údajov, ktorú majú tieto technológie, exponenciálne vzrástla,
- nové formy spracúvania, napríklad týkajúce sa osobných údajov o používaní online služieb a/alebo lokalizačných údajov pochádzajúcich z inteligentného zariadenia, sú pre zamestnancov oveľa menej viditeľné než iné, tradičnejšie typy, ako verejné kamery priemyselnej televízie. To vyvoláva otázky o miere, do akej si zamestnanci uvedomujú tieto technológie, keďže zamestnávatelia môžu nezákonne zaviesť takéto spracúvanie bez predchádzajúceho oznámenia zamestnancom a
- hranice medzi domovom a prácou sa čoraz viac rozmazávajú. Napríklad keď zamestnanci pracujú na diaľku (napr. z domu), resp. sú na pracovnej ceste, môže dochádzať k monitorovaniu činností mimo fyzického pracovného prostredia a toto monitorovanie môže zahŕňať monitorovanie jednotlivcov v súkromnom prostredí.

Hoci použitie týchto technológií môže byť užitočné pri odhaľovaní alebo predchádzaní stratám duševného a materiálneho vlastníctva spoločnosti, pri zvyšovaní produktivity zamestnancov a ochrane osobných údajov, za ktoré zodpovedá prevádzkovateľ, vznikajú pri ňom aj značné problémy s ochranou súkromia a osobných údajov. V dôsledku toho je potrebné vykonať nové posúdenie týkajúce sa rovnováhy medzi oprávneným záujmom zamestnávateľa chrániť svoje podnikanie a odôvodnenými očakávaniami súvisiacimi so súkromím dotknutých osôb: zamestnancov.

Hoci sa toto stanovisko zameria na nové informačné technológie prostredníctvom posúdenia deviatich rôznych scenárov, v ktorých sa môžu použiť, stručne sa zaoberá aj tradičnejšími metódami spracúvania údajov v práci, pri ktorých sú riziká v dôsledku technologickej zmeny väčšie.

Keď sa v tomto stanovisku používa slovo „zamestnanec“, pracovná skupina zriadená podľa článku 29 nemá v úmysle zužovať rozsah tohto pojmu iba na osoby s pracovnou zmluvou uznanou za pracovnú zmluvu podľa platného pracovného práva. V predchádzajúcich desaťročiach sa bežnými stali nové obchodné modely založené na rozličných typoch pracovnoprávnych vzťahov, a najmä zamestnávanie na živnostenské oprávnenie. Toto stanovisko má pokrývať všetky situácie so zamestnaneckým vzťahom bez ohľadu na to, či je tento vzťah založený na pracovnej zmluve.

Treba uviesť, že zamestnanci len zriedka môžu slobodne udeliť, zamietnuť alebo zrušiť súhlas vzhľadom na závislosť vyplývajúcu zo vzťahu medzi zamestnávateľom a zamestnancom. Pokiaľ nejde o výnimočné situácie, musia sa zamestnávatelia opierať o iný právny dôvod než súhlas – napríklad o potrebu spracúvať údaje z dôvodu ich oprávneného záujmu. Samotný oprávnený záujem však nie je dostatočný dôvod na potlačenie práv a slobôd zamestnancov.

Bez ohľadu na právny základ takéhoto spracúvania by sa pred začiatkom spracúvania mal uskutočniť test proporcionality, aby sa posúdilo, či je spracúvanie nevyhnutné na dosiahnutie legitímneho účelu, ako aj na posúdenie opatrení, ktoré sa musia prijať s cieľom zabezpečiť čo najväčšie obmedzenie porušení práv na súkromný život a dôvernosť komunikácie. Tento test môže byť súčasťou posúdenia vplyvu na ochranu údajov.

3. Právny rámec

Hoci analýza uvedená ďalej sa uskutočnila predovšetkým vo vzťahu k súčasnému právnemu rámcu podľa smernice 95/46/EHS (smernica o ochrane údajov)[3], toto stanovisko je zamerané aj na povinnosti vyplývajúce z nariadenia (EÚ) 2016/679 (všeobecné nariadenie o ochrane údajov)[4], ktoré už nadobudlo účinnosť a ktoré sa začne uplatňovať 25. mája 2018.

Pokiaľ ide o navrhované nariadenie o ochrane súkromia v elektronickej komunikácii[5], pracovná skupina vyzýva európskych zákonodarcov, aby vytvorili osobitnú výnimku pre zasahovanie do zariadení poskytnutých zamestnancom[6]. Navrhované nariadenie neobsahuje vhodnú výnimku pre všeobecný zákaz zasahovania a zamestnávatelia zvyčajne nemôžu zabezpečiť platný súhlas svojich zamestnancov na spracúvanie osobných údajov.

3.1. Smernica 95/46/EHS – smernica o ochrane údajov

V stanovisku č. 8/2001 pracovná skupina zriadená podľa článku 29 v minulosti uviedla, že zamestnávatelia pri spracúvaní osobných údajov v súvislosti s pracovným pomerom zohľadňujú základné zásady ochrany osobných údajov smernice o ochrane údajov. Vývojom nových technológií a nových metód spracúvania v tejto súvislosti sa táto situácia nezmenila. V skutočnosti možno povedať, že takýto vývoj *zvýšil* význam toho, aby tak zamestnávatelia robili. V tejto súvislosti by zamestnávatelia:

- mali zabezpečiť, že údaje sa budú spracúvať na konkrétne a legitímne účely, ktoré sú primerané a nevyhnutné,
- mali zohľadniť zásadu obmedzenia účelu, pričom zároveň zabezpečia, že údaje budú primerané, relevantné a nebudú neprimerané na svoj legitímny účel,
- mali uplatniť zásady proporcionality a subsidiarity bez ohľadu na platný právny dôvod,
- mali byť transparentní voči zamestnancom, pokiaľ ide o použitie a účely technológií monitorovania,
- mali zabezpečiť uplatňovanie práv dotknutých osôb vrátane práva na prístup k údajom a podľa potreby práva na opravu, práva na vymazanie alebo blokovanie osobných údajov,
- mali zachovávať správnosť údajov a nemali by ich uchovávať dlhšie, než je nevyhnutné, a
- mali prijať všetky potrebné opatrenia na ochranu údajov pred neoprávneným prístupom a zabezpečiť, aby si zamestnanci dostatočne uvedomovali povinnosti v oblasti ochrany osobných údajov.

---

[3] Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, *Ú. v. ES L 281, 23.11.1995, s. 31 – 50*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), *Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[5] Návrh nariadenia Európskeho parlamentu a Rady o rešpektovaní súkromného života a ochrane osobných údajov v elektronických komunikáciách a o zrušení smernice 2002/58/ES, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] Pozri pracovná skupina zriadená podľa článku 29, *Stanovisko č. 1/2017 k navrhovanému nariadeniu o súkromí a elektronických komunikáciách*, WP 247, 4. apríla 2017, strana 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

Bez opakovania poradenstva poskytnutého v minulosti by pracovná skupina zriadená podľa článku 29 chcela poukázať na tri zásady, a to konkrétne: právne dôvody, transparentnosť a automatizované rozhodnutia.

3.1.1. *PRÁVNE DÔVODY (ČLÁNOK 7)*

Pri spracúvaní osobných údajov v súvislosti s pracovným pomerom musí byť splnené aspoň jedno z kritérií stanovených v článku 7. Ak typy spracúvaných osobných údajov zahŕňajú osobitné kategórie (ako sa uvádza v článku 8), spracúvanie je zakázané, okrem prípadov, na ktoré sa vzťahuje výnimka[7,8]. Aj vtedy, ak sa zamestnávateľ môže odvolať na jednu z týchto výnimiek, stále je pre legitímnosť spracúvania potrebné splnenie právneho dôvodu z článku 7.

Celkovo si teda zamestnávatelia musia všimnúť:

- že v prípade väčšiny podobného spracúvania údajov v práci **právnym základom nemôže a nemal by byť súhlas zamestnancov** [článok 7 písm. a)] z dôvodu povahy vzťahu medzi zamestnávateľom a zamestnancom,
- že spracúvanie môže byť potrebné pre **plnenie zmluvy** [článok 7 písm. b)] v prípadoch, keď zamestnávateľ musí spracovať osobné údaje zamestnanca na splnenie týchto povinností,
- že je celkom bežné, že v **pracovnom práve sa môžu zaviesť právne záväzky** [článok 7 písm. c)]**, ktoré si vyžadujú spracúvanie osobných údajov**; v týchto prípadoch sa zamestnanec musí jasne a v plnej miere informovať o tomto spracúvaní (pokiaľ sa neuplatňuje výnimka),
- že pokiaľ sa zamestnávateľ odvoláva na **oprávnený záujem** [článok 7 písm. f)], účel spracúvania musí byť legitímny; zvolená metóda alebo osobitná technológia musí byť nevyhnutná, primeraná a musí sa zaviesť čo najmenej rušivým spôsobom a musí byť schopná umožniť zamestnávateľovi preukázať, že **sa zaviedli primerané opatrenia** na zabezpečenie vyváženia so základnými právami a slobodami zamestnancov[9],
- že aj spracovateľské operácie musia spĺňať **požiadavky na transparentnosť** (články 10 a 11) a zamestnanci by sa mali jasne a v plnej miere informovať o spracúvaní ich osobných údajov[10], ako aj o existencii akéhokoľvek monitorovania, a
- že by sa mali prijať **príslušné technické a organizačné opatrenia** na zaistenie bezpečnosti spracúvania (článok 17).

Najrelevantnejšie kritériá podľa článku 7 sa podrobne uvádzajú ďalej.

- **Súhlas [článok 7 písm. a)]**

[7] Ako sa uvádza v časti 8 stanoviska č. 8/2001; napríklad v článku 8 ods. 2 písm. b) sa stanovuje výnimka na účely vykonávania záväzkov a špecifických práv kontrolóra v oblasti pracovného práva, pokiaľ je autorizované vnútroštátnym právom zabezpečujúcim adekvátne záruky.

[8] Treba pripomenúť, že v niektorých krajinách platia osobitné opatrenia, ktoré musia zamestnávatelia dodržiavať na účely ochrany súkromného života zamestnancov. Portugalsko je príkladom krajiny, v ktorej existujú takéto osobitné opatrenia a podobné opatrenia sa môžu uplatňovať aj v ďalších členských štátoch. Závery v oddiele 5.6, ako aj príklady uvedené v oddieloch 5.1 a 5.7.1 tohto stanoviska, teda z týchto dôvodov neplatia v Portugalsku.

[9] Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 6/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES*, WP 217, prijaté 9. apríla 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[10] Podľa článku 11 ods. 2 smernice o ochrane údajov je prevádzkovateľ vyňatý z povinnosti informovať dotknutú osobu v prípadoch, keď je v zákone výslovne stanovené zaznamenanie alebo zber údajov.

Súhlas je podľa smernice o ochrane údajov vymedzený ako slobodne poskytnutá a informovaná indikácia prianí dotknutej osoby, ktorou prejaví svoj súhlas, aby sa osobné údaje, ktoré sa jej týkajú, spracovali. Na to, aby bol súhlas platný, musí byť aj odvolateľný.

Pracovná skupina zriadená podľa článku 29 v minulosti v stanovisku č. 8/2001 uviedla, že v prípade, ak zamestnávateľ musí spracúvať osobné údaje svojich zamestnancov, je chybné začínať predpokladom, že spracúvanie možno legitimizovať súhlasom zamestnancov. V prípadoch, keď zamestnávateľ tvrdí, že potrebuje súhlas, a keď existuje reálna alebo možná závažná ujma vyplývajúca z toho, že zamestnanec nedá svoj súhlas so spracúvaním (čo môže byť veľmi pravdepodobné v súvislosti s pracovným pomerom, najmä ak sa táto ujma týka toho, že zamestnávateľ sleduje správanie zamestnanca), potom je tento súhlas neplatný, pretože nebol a nemohol byť vydaný slobodne. Vo väčšine prípadov spracúvania údajov zamestnancov teda právnym základom tohto spracúvania nemôže a nemá byť súhlas zamestnancov, takže je potrebný iný právny základ.

Okrem toho aj v prípadoch, keď by sa súhlas mohol považovať za platný právny základ takéhoto spracúvania (t. j. ak možno bez pochybností dospieť k záveru, že súhlas bol daný slobodne), tento súhlas musí byť konkrétnou a informovanou indikáciou prianí zamestnanca. Štandardné nastavenia na zariadeniach a/alebo inštalovaného softvéru, ktoré uľahčujú spracúvanie elektronických osobných údajov, nemožno považovať za súhlas zamestnanca, pretože na súhlas je potrebné aktívne vyjadrenie vôle. Nedostatok činnosti (t. j. skutočnosť, že neboli zmenené štandardné nastavenia) nemožno vo všeobecnosti považovať za špecifický súhlas umožňujúci takéto spracúvanie[11].

- **Plnenie zmluvy [článok 7 písm. b)]**

Pracovnoprávne vzťahy sa často zakladajú pracovnou zmluvou medzi zamestnávateľom a zamestnancom. Pri plnení povinností podľa tejto zmluvy, ako je napr. výplata zamestnancov, musí zamestnávateľ spracúvať určité osobné údaje.

- **Právne záväzky [článok 7 písm. c)]**

Je celkom bežné, že v pracovnom práve sa zamestnávateľovi stanovujú právne záväzky, ktoré si vyžadujú spracúvanie osobných údajov (napr. na účely výpočtu dane a mzdovej správy). V takýchto prípadoch toto právo jasne predstavuje právny základ na spracúvanie osobných údajov.

- **Oprávnený záujem [článok 7 písm. f)]**

Ak sa zamestnávateľ chce odvolávať na právny dôvod podľa článku 7 písm. f) smernice o ochrane údajov, účel spracúvania musí byť legitímny a zvolená metóda alebo osobitná technológia, ktorou sa má spracúvanie vykonať, musí byť nevyhnutná pre oprávnený záujem zamestnávateľa. Spracúvanie musí byť takisto primerané podnikateľským potrebám, t. j. účelu, na ktorý je určené. Spracúvanie údajov v práci by sa malo vykonávať čo najmenej rušivým spôsobom a malo by byť zamerané na konkrétnu oblasť rizika. Navyše, ak sa spracúvanie odvoláva na článok 7 písm. f), zamestnanec si ponecháva právo namietať proti spracúvaniu z nevyvrátiteľných zákonných dôvodov podľa článku 14.

[11] Pozri aj pracovná skupina zriadená podľa článku 29, *Stanovisko č. 15/2011 k definícii súhlasu*, WP 187, 13. júla 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, strana 24.

Na uplatnenie článku 7 písm. f) ako právneho dôvodu na spracúvanie je podstatné, aby boli zavedené osobitné zmierňujúce opatrenia na zabezpečenie správnej rovnováhy medzi oprávneným záujmom zamestnávateľa a základnými právami a slobodami zamestnancov[12]. Tieto opatrenia by v závislosti od formy monitorovania mali zahŕňať obmedzenia monitorovania, aby sa zaručilo, že nedôjde k narušeniu súkromia zamestnanca. Mohlo by ísť o takéto obmedzenia:

- geografické obmedzenia (napr. monitorovanie iba v konkrétnych miestach; monitorovanie citlivých priestorov, ako sú miesta náboženského stretávania a napríklad hygienické priestory a miestnosti na prestávky, by sa malo zakázať),
- obmedzenia zamerané na údaje (napr. osobné elektronické súbory a komunikácia by sa nemali monitorovať) a
- časové obmedzenia (napr. odber vzoriek namiesto súvislého monitorovania).

3.1.2. *TRANSPARENTNOSŤ (ČLÁNKY 10 A 11)*

Na spracúvanie údajov v práci sa vzťahujú požiadavky na transparentnosť podľa článkov 10 a 11. Zamestnancom sa musia poskytnúť informácie o každom monitorovaní, účeloch, na ktoré sa majú spracúvať osobné údaje, a všetky ďalšie informácie potrebné na zaručenie spravodlivého spracúvania.

S novými technológiami sa potreba transparentnosti stala zrejmejšou, pretože umožňujú zber a ďalšie spracúvanie pravdepodobne obrovských množstiev osobných údajov skrytým spôsobom.

3.1.3. *AUTOMATIZOVANÉ ROZHODNUTIA (ČLÁNOK 15)*

Článkom 15 smernice o ochrane údajov sa dotknutým osobám zaručuje právo, aby neboli závislé od rozhodnutia, ktoré je založené výhradne na automatizovanom spracúvaní údajov, ak má toto rozhodnutie právne účinky alebo má na dotknuté osoby podobne závažný vplyv a ktoré je založené výhradne na automatizovanom spracúvaní údajov určených na hodnotenie určitých osobných vlastností, ako je výkonnosť v práci, pokiaľ toto rozhodnutie nie je nevyhnutné na uzatvorenie zmluvy či na jej plnenie, pokiaľ nie je povolené právom Únie alebo členského štátu, alebo pokiaľ nie je založené na výslovnom súhlase dotknutej osoby.

3.2. Nariadenie (EÚ) 2016/679 – všeobecné nariadenie o ochrane údajov

Všeobecné nariadenie o ochrane údajov obsahuje a posilňuje požiadavky smernice o ochrane údajov. Zavádzajú sa ním aj nové povinnosti pre všetkých prevádzkovateľov vrátane zamestnávateľov.

3.2.1. *ŠPECIFICKY NAVRHNUTÁ OCHRANA ÚDAJOV*

[12] Príklad rovnováhy, ktorú treba dosiahnuť, sa uvádza vo veci *Köpke/Nemecko*, [2010] ESĽP 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), ktorej predmetom bolo prepustenie zamestnanca na základe skrytého monitorovania kamerovým systémom, ktoré vykonával zamestnávateľ a súkromná detektívna agentúra. Hoci súd v tomto prípade dospel k záveru, že domáce orgány dosiahli spravodlivú rovnováhu medzi oprávneným záujmom zamestnávateľa (pri ochrane jeho vlastníckych práv), právom zamestnanca na rešpektovanie súkromného života a verejným záujmom pri výkone spravodlivosti, poznamenal aj, že rozličné záujmy by v budúcnosti mohli mať v dôsledku technického vývoja rozdielnu váhu.

Podľa článku 25 všeobecného nariadenia o ochrane údajov sa od prevádzkovateľov vyžaduje, aby prijali špecificky navrhnutú a štandardnú ochranu údajov. Napríklad: ak zamestnávateľ zamestnancom rozdá zariadenia, ak sa v nich nachádzajú sledovacie technológie, treba vybrať riešenia, ktoré viac zohľadňujú ochranu súkromia. Zohľadniť sa musí aj minimalizácia údajov.

3.2.2. *POSÚDENIA VPLYVU NA OCHRANU ÚDAJOV*

V článku 35 všeobecného nariadenia o ochrane údajov sa opisujú požiadavky pre prevádzkovateľov na vykonávanie posúdenia vplyvu na ochranu údajov, kde typ spracúvania, konkrétne pri používaní nových technológií a s ohľadom na povahu, rozsah, kontext a účely samotného spracúvania, môže viesť k vysokému riziku pre práva a slobody fyzických osôb. Príkladom je prípad systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu.

Ak sa v posúdení vplyvu na ochranu údajov uvádza, že zistené riziká nemôže prevádzkovateľ dostatočne riešiť, t. j. že zvyškové riziká sú stále vysoké, potom prevádzkovateľ musí pred začiatkom spracúvania uskutočniť konzultácie s dozorným orgánom (článok 36 ods. 1), ako sa objasňuje v usmerneniach pracovnej skupiny zriadenej podľa článku 29 o posúdeniach vplyvu na ochranu údajov[13].

3.2.2. *„SPRACÚVANIE V SÚVISLOSTI SO ZAMESTNANÍM“*

V článku 88 všeobecného nariadenia o ochrane údajov sa uvádza, že členské štáty môžu prostredníctvom právnych predpisov alebo kolektívnych dohôd stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním. Tieto pravidlá sa môžu stanoviť najmä na účely:

- prijatia do zamestnania,
- plnenia pracovnej zmluvy (vrátane plnenia povinností vyplývajúcich z právnych predpisov alebo kolektívnych zmlúv),
- riadenia, plánovania a organizácie práce,
- rovnosti a rozmanitosti na pracovisku,
- ochrany zdravia a bezpečnosti pri práci,
- ochrany majetku zamestnávateľa alebo zákazníka,
- uplatňovania a využívania práv a výhod (na individuálnom základe) súvisiacich so zamestnaním a
- ukončenia pracovného pomeru.

V súlade s článkom 88 ods. 2 by všetky uvedené pravidlá mali zahŕňať vhodné a osobitné opatrenia na zaistenie ľudskej dôstojnosti, oprávnených záujmov a základných práv dotknutej osoby s osobitným zameraním na:

- transparentnosť spracúvania,

[13] Pracovná skupina zriadená podľa článku 29, *Usmernenia o posúdení vplyvu na ochranu údajov a o určovaní, či spracúvanie môže viesť k „vysokému riziku“, na účely nariadenia (EÚ) 2016/679*, WP 248, 4. apríla 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, strana 18.

- prenos osobných údajov v rámci skupiny podnikov alebo podnikov zapojených do spoločnej hospodárskej činnosti a
- systémy monitorovania na pracovisku.

V tomto stanovisku pracovná skupina poskytla usmernenia na oprávnené použitie nových technológií v niekoľkých osobitných situáciách, pričom podrobne uviedla vhodné a osobitné opatrenia na zaistenie ľudskej dôstojnosti, oprávnených záujmov a základných práv zamestnancov.

4. Riziká

Moderné technológie umožňujú sledovať zamestnancov v čase, na pracoviskách a v ich domovoch, prostredníctvom množstva rozličných zariadení, ako sú smartfóny, stolové počítače, tabletové počítače, vozidlá a nositeľné zariadenia. Ak neexistujú hranice spracúvania a ak nie je transparentné, existuje vysoké riziko, že oprávnený záujem zamestnávateľov o zvýšenie efektívnosti a ochranu majetku spoločnosti sa premení na neoprávnené a obťažujúce monitorovanie.

Technológie, ktoré monitorujú komunikácie, môžu mať aj nepriaznivý účinok na základné práva zamestnancov organizovať sa, usporadúvať stretnutia pracovníkov a komunikovať v dôvernosti (vrátane práva vyhladávať informácie). Monitorovaním komunikácie a správania vzniká tlak na zamestnancov na podriadenie sa s cieľom zabrániť tomu, čo by sa mohlo chápať ako anomálie, a to spôsobom, ktorý je porovnateľný so spôsobom, akým intenzívne používanie kamerového systému ovplyvnilo správanie občanov vo verejných priestoroch. Okrem toho si z dôvodu schopností týchto technológií zamestnanci nemusia uvedomovať, ktoré osobné údaje sa spracúvajú a na aké účely, a zároveň je možné, že ani nevedia o existencii samotnej monitorovacej techniky.

Monitorovanie používania informačných technológií sa takisto odlišuje od iných, zreteľnejších nástrojov na pozorovanie a monitorovanie, ako je kamerový systém, a to v tom zmysle, že môže prebiehať skrytým spôsobom. Ak neexistuje ľahko zrozumiteľná a rýchlo dostupná politika monitorovania na pracovisku, zamestnanci nemusia vedieť o existencii a následkoch monitorovania, ku ktorému dochádza, a preto nemôžu uplatňovať svoje práva. Ďalšie riziká vyplývajú z „nadmerného zberu“ údajov v týchto systémoch, napr. systémoch na zber lokalizačných údajov z WiFi.

Zvýšenie množstva údajov získaných na pracovisku v spojení s novými spôsobmi analýzy údajov a hľadania zhody môže takisto vytvárať riziká nezlučiteľného ďalšieho spracúvania. Medzi príklady nezákonného ďalšieho spracúvania patrí používanie systémov, ktoré sú legitímne inštalované na ochranu majetku na monitorovanie dostupnosti zamestnancov, ich výkonnosti a spokojnosti zákazníkov so zamestnancami. Ďalším príkladom je používanie údajov zozbieraných prostredníctvom kamerového systému na pravidelné monitorovanie správania a výkonnosti zamestnancov alebo používanie údajov systému na určovanie geografickej polohy (napríklad sledovanie WiFi alebo bluetooth) na neustále sledovanie pohybu a správania zamestnanca.

Vo výsledku môže toto sledovanie narušovať právo zamestnancov na súkromie bez ohľadu na to, či k monitorovaniu dochádza systematicky alebo príležitostne. Riziko sa netýka iba

analýzy obsahu komunikácie. Analýza metaúdajov o osobe tak môže umožniť rovnako podrobné monitorovanie života jednotlivca a vzorov jeho správania, ktoré narúša súkromie.

Rozsiahle používanie monitorovacích technológií môže obmedziť aj ochotu zamestnancov (a spôsoby, ktorými by mohli) informovať zamestnávateľov o nezrovnalostiach alebo nezákonnom konaní nadriadených a/alebo iných zamestnancov, ktoré hrozia poškodením podnikania (najmä údajov klientov) alebo pracoviska. Príslušný zamestnanec často potrebuje anonymitu na to, aby konal a takéto situácie nahlásil. Monitorovanie, ktoré narúša práva zamestnancov na súkromie, môže brániť potrebnej komunikácii s príslušnými úradníkmi. V takom prípade sa dostupné prostriedky pre interných informátorov môžu stať neúčinné[14].

5. Scenáre

Táto časť je venovaná niekoľkým scenárom spracúvania údajov v práci, v ktorých nové technológie a/alebo vývoj existujúcich technológií má alebo môže mať potenciál spôsobiť vysoké riziká pre súkromie zamestnancov. Vo všetkých týchto prípadoch by zamestnávatelia mali posúdiť:

- či je spracovateľská činnosť nevyhnutná, a pokiaľ áno, právne dôvody, ktoré sa uplatňujú,
- či je navrhované spracúvanie osobných údajov spravodlivé voči zamestnancom,
- či je spracovateľská činnosť primeraná vyvolaným problémom, a
- či je spracovateľská činnosť transparentná.

5.1. Spracovateľské operácie počas prijímania do zamestnania

Používanie sociálnych médií jednotlivcami je všeobecne rozšírené a je pomerne bežné, aby bolo možné používateľské profily verejne prezerať v závislosti od nastavení, ktoré si zvolil držiteľ účtu. V dôsledku toho môžu byť zamestnávatelia presvedčení, že prezeranie sociálnych profilov perspektívnych uchádzačov počas prijímacích pohovorov môže byť oprávnené. To môže platiť aj v prípade iných verejne dostupných informácií o potenciálnom zamestnancovi.

Zamestnávatelia by však nemali predpokladať, že iba z dôvodu, že profil daného jednotlivca na sociálnych médiách je verejne dostupný, môžu spracúvať tieto údaje na svoje vlastné účely. Na toto spracúvanie je potrebný právny dôvod, ako je oprávnený záujem. V tejto súvislosti by zamestnávateľ mal pred preskúmaním profilu na sociálnych médiách zohľadniť, či profil uchádzača na sociálnych médiách súvisí s pracovným alebo súkromným účelom, pretože to môže byť dôležitým príznakom pre právnu prípustnosť kontroly údajov. Zamestnávatelia okrem toho môžu zbierať a spracúvať osobné údaje týkajúce sa uchádzačov o prácu iba v miere, v akej je zber týchto údajov potrebný a podstatný pre výkon zamestnania, o ktoré sa uchádzajú.

[14] Pozri napríklad pracovná skupina zriadená podľa článku 29, *Stanovisko č. 1/2006 k problematike uplatňovania noriem EÚ o ochrane údajov na vnútorné mechanizmy oznamovania podozrení z nekalého konania (whistleblowing) v oblasti účtovníctva, vnútorných účtovných kontrol, auditu, boja proti úplatkárstvu a trestnej činnosti v bankovom a finančnom sektore*, WP 117, 1. februára 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

Údaje získané počas prijímania pracovníkov by sa mali vo všeobecnosti vymazať hneď, keď bude jasné, že sa príslušnému uchádzačovi ponúkne zamestnanie alebo že uchádzač túto ponuku odmietne[15]. Pred tým, než sa jednotlivec zúčastní na prijímacom procese, musí byť správne informovaný o každom takomto spracúvaní.

Neexistuje právny dôvod, na základe ktorého zamestnávateľ môže od potenciálnych zamestnancov požadovať, aby si potenciálneho zamestnávateľa „pridali medzi priateľov“ alebo iným spôsobom poskytli prístup k obsahu svojich profilov.

Príklad

Počas prijímania nových zamestnancov zamestnávateľ preveruje profily uchádzačov na rôznych sociálnych sieťach a informácie z týchto sietí (a všetky ďalšie informácie, ktoré sú k dispozícii na internete) zahrnie do procesu preverovania.

Zamestnávateľ môže uplatniť právny základ podľa článku 7 písm. f) na preskúmanie verejne dostupných informácií o uchádzačoch iba vtedy, ak je pre pracovnú pozíciu nevyhnutné preskúmať informácie o uchádzačovi na sociálnych médiách, napríklad na to, aby bolo možné posúdiť osobitné riziká týkajúce sa uchádzačov o konkrétnu funkciu, a ak sa uchádzači správne informujú (napríklad v rámci textu pracovného inzerátu).

[15] Pozri aj Rada Európy, *Odporúčanie CM/Rec(2015)5 Výboru ministrov pre členské štáty o spracúvaní osobných údajov v súvislosti so zamestnaním*, bod 13.2 (1. apríla 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). V prípadoch, keď chce zamestnávateľ uchovať údaje vzhľadom na ďalšiu pracovnú príležitosť, dotknutá osoba sa má o tom informovať a má sa jej dať možnosť vzniesť námietky proti takémuto ďalšiemu spracúvaniu a v takom prípade by sa údaje mali vymazať (Tamže).

5.2. Spracovateľské operácie vyplývajúce z preverovania v rámci zamestnania

Prostredníctvom profilov na sociálnych médiách a vývoja nových analytických technológií zamestnávatelia majú (alebo môžu získať) technickú schopnosť trvalo preverovať zamestnancov zberom informácií týkajúcich sa ich priateľov, názorov, presvedčení, záujmov, zvykov, miest pobytu, postojov a správania, a teda schopnosť získavať údaje vrátane citlivých údajov súvisiacich so súkromným a rodinným životom zamestnanca.

Preverovanie profilov zamestnancov na sociálnych médiách v zamestnaní by nemalo byť všeobecné.

Zamestnávatelia by okrem toho od zamestnanca alebo uchádzača o prácu nemali požadovať prístup k informáciám, o ktoré sa delí s inými osobami prostredníctvom sociálnych sietí.

Príklad
Zamestnávateľ monitoruje profily na sieti LinkedIn, ktoré sa týkajú bývalých zamestnancov počas platnosti doložiek o zákaze konkurencie. Účelom tohto monitorovania je monitorovať dodržiavanie týchto doložiek. Monitoring sa týka iba bývalých zamestnancov.

Pokiaľ zamestnávateľ môže dokázať, že monitorovanie je potrebné na ochranu jeho oprávnených záujmov, že k dispozícii nie sú iné, menej invazívne prostriedky a že bývalých zamestnancov primerane informoval o rozsahu pravidelného pozorovania ich verejnej komunikácie, zamestnávateľ sa bude môcť odvolávať na právny základ článku 7 písm. f) smernice o ochrane údajov.

Zamestnanci by navyše nemali mať povinnosť používať profil na sociálnych médiách, ktorý vytvoril ich zamestnávateľ. Aj keby bola táto povinnosť osobitne stanovená vzhľadom na ich úlohy (napr. hovorca organizácie), musia mať možnosť používať „mimopracovný“ neverejný profil, ktorý môžu používať namiesto „oficiálneho“ profilu od zamestnávateľa, čo by sa malo uviesť v podmienkach pracovnej zmluvy.

5.3. Spracovateľské operácie vyplývajúce z monitorovania používania IKT na pracovisku

Tradične sa monitorovanie elektronických komunikácií na pracovisku (napr. telefón, prezeranie internetu, e-mail, služby rýchlych správ, VOIP atď.) považovalo za významnú hrozbu pre súkromie zamestnancov. Pracovná skupina zriadená podľa článku 29 vo svojom *pracovnom dokumente o dohľade nad elektronickými komunikáciami na pracovisku* z roku 2001 dospela k niekoľkým záverom týkajúcim sa monitorovania e-mailovej komunikácie a používania internetu. Hoci tieto závery stále platia, je potrebné zohľadniť technický vývoj, ktorý umožnil novšie, potenciálne viac obťažujúce a prenikavejšie spôsoby monitorovania. Medzi výsledky tohto vývoja okrem iného patria:

- nástroje na ochranu pred únikom údajov (DLP), ktoré monitorujú komunikáciu smerujúcu von na účely odhalenia možných porušení ochrany údajov,
- Brány firewall nasledujúcej generácie (NGFW) a systémy jednotného zvládania ohrozenia (UTM), ktoré poskytujú rozličné technológie monitorovania vrátane hĺbkovej analýzy paketov, odpočúvania komunikácie protokolu TLS, filtrovania webového sídla, filtrovania obsahu, podávania správ v zariadení, informácií o totožnosti používateľa a (ako už bolo uvedené) ochrany pred únikom údajov. Tieto

technológie sa môžu zaviesť aj individuálne, v závislosti od rozhodnutia zamestnávateľa,

- bezpečnostné aplikácie a opatrenia, ktorých súčasťou je zaznamenávanie prístupu zamestnancov do systémov zamestnávateľa,
- technológia nakladania s dôkazmi v elektronickej podobe (eDiscovery), ktorá sa týka každého postupu, pri ktorom sa prehľadávajú elektronické údaje s cieľom použiť tieto údaje ako dôkaz,
- sledovanie používania aplikácií a zariadení prostredníctvom nevideného softvéru, či už na stolovom počítači, alebo v rámci cloudu,
- používanie kancelárskych aplikácií na pracovisku, ktoré sa poskytujú v rámci cloudových služieb a ktoré teoreticky umožňujú veľmi podrobné zaznamenávanie činností zamestnancov,
- monitorovanie osobných zariadení (napr. osobných počítačov, mobilných telefónov, tabletových počítačov), ktoré zamestnanci prinášajú do svojej práce v súlade s politikou osobitného použitia, napríklad zásada „prines si vlastné zariadenie“ (Bring-Your-Own-Device, BYOD), ako aj technológia správy mobilných zariadení (Mobile Device Management, MDM), ktorá umožňuje distribuovať aplikácie, údaje a konfiguračné nastavenia a opráv pre mobilné zariadenia a
- použitie nositeľných zariadení (napr. zariadenia na sledovanie zdravotného stavu a fyzickej zdatnosti).

Môže sa stať, že zamestnávateľ zavedie integrované riešenie monitorovania, ako je súbor balíkov bezpečnostných aplikácií, ktoré mu umožňujú monitorovať všetko používanie IKT na pracovisku na rozdiel od monitorovania iba e-mailovej komunikácie a/alebo webového sídla, ktoré sa uskutočňovalo v minulosti. Závery prijaté v dokumente WP 55 sa uplatňujú na každý systém, ktorý umožňuje vykonávať takéto monitorovanie[16].

Príklad

Zamestnávateľ plánuje zaviesť zariadenie na kontrolu protokolu TLS na dešifráciu a kontrolu zabezpečenej aktivity s cieľom odhaliť akúkoľvek škodlivú komunikáciu. Zariadenie dokáže aj zaznamenávať a analyzovať aktivitu zamestnanca online na sieti organizácie v jej celistvosti.

Použitie šifrovaných komunikačných protokolov sa čoraz častejšie zavádza na ochranu tokov online údajov týkajúcich sa osobných údajov pred odpočúvaním. To však môže takisto predstavovať problémy, keďže šifrovanie znemožňuje monitorovanie prichádzajúcich a odchádzajúcich údajov. Vybavenie na kontrolu protokolu TLS dešifruje dátový tok, analyzuje obsah na účely bezpečnosti, a potom dátový tok znovu šifruje.

V tomto príklade sa zamestnávateľ odvoláva na oprávnené záujmy, potrebu chrániť sieť a osobné údaje zamestnancov a zákazníkov uchovávaných na tejto sieti proti neoprávnenému prístupu alebo úniku údajov. Monitorovanie každej aktivity zamestnancov na internete však predstavuje neprimeranú reakciu a zásah do práva na dôvernosť komunikácie. Zamestnávateľ

[16] Pozri aj vec *Copland/Spojené kráľovstvo,* (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ESĽP 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), v ktorej súd uviedol, že e-maily odoslané z prevádzkových priestorov a informácie odvodené z monitorovania používania internetu by mohli tvoriť súčasť súkromného života a korešpondencie zamestnanca a že zber a uchovávanie týchto informácií bez vedomia zamestnanca predstavujú porušenie práv zamestnanca, hoci súd nerozhodol, že takéto monitorovanie nemôže byť v demokratickej spoločnosti nikdy potrebné.

by mal najprv preskúmať iné, menej invazívne prostriedky na ochranu dôvernosti údajov zákazníkov a bezpečnosti siete.

V miere, v akej možno odpočúvanie aktivity v rámci TLS posúdiť ako jednoznačne nevyhnutné, by sa zariadenie malo nastaviť tak, aby sa zabránilo neustálemu zaznamenávaniu aktivít zamestnancov, napríklad zablokovaním podozrivej prichádzajúcej a odchádzajúcej prevádzky a presmerovaním používateľa na informačný portál, na ktorom môže požiadať o preskúmanie tohto automatizovaného rozhodnutia. Ak sa určité všeobecné zaznamenávanie bude považovať za jednoznačne nevyhnutné, zariadenie sa môže nastaviť tak, aby neuchovávalo údaje z denníka, s výnimkou prípadu, keď zariadenie signalizuje výskyt incidentu, pričom sa minimalizujú zhromažďované informácie.

Ako osvedčený postup by zamestnávateľ mohol zamestnancom ponúkať alternatívny nemonitorovaný prístup. Tento cieľ by sa mohol uskutočniť ponukou bezplatného pripojenia WiFi alebo samostatných zariadení či terminálov (s primeranými zárukami na zabezpečenie dôvernosti správ), prostredníctvom ktorých môžu zamestnanci uplatniť svoje zákonné právo použiť pracovné zariadenia na určité súkromné účely[17]. Zamestnávatelia by okrem toho mali zvážiť určité typy prevádzky, ktorých odpočúvanie ohrozuje správnu rovnováhu medzi ich oprávnenými záujmami a súkromím zamestnancov (ako je používanie súkromnej webmailovej služby, návštevy služieb elektronického bankovníctva a webových sídel zdravotníckych zariadení), s cieľom primerane nastaviť zariadenie tak, aby sa nepokračovalo v odpočúvaní komunikácie v situáciách, ktoré porušujú zásadu proporcionality. Informácie o type komunikácie, ktoré zariadenie monitoruje, by sa mali výslovne oznámiť zamestnancom.

Mala by sa vypracovať politika týkajúca sa účelov, kedy a kto môže mať prístup k podozrivým údajom z denníka, a všetci zamestnanci by k tejto politike mali mať ľahký a trvalý prístup, aby sa ňou mohli riadiť, pokiaľ ide o prijateľné a neprijateľné používanie siete a zariadení. To zamestnancom umožňuje prispôsobiť svoje správanie tak, aby zabránili svojmu monitorovaniu, keď oprávnene používajú pracovné informačné technológie na súkromné použitie. V rámci osvedčeného postupu by sa táto politika mala aspoň raz za rok vyhodnotiť s cieľom posúdiť, či zvolené riešenie monitorovania dosahuje plánované výsledky a či existujú iné, menej invazívne nástroje alebo prostriedky na dosiahnutie rovnakých účelov.

Bez ohľadu na príslušnú technológiu alebo jej schopnosti je právny základ podľa článku 7 písm. f) k dispozícii iba vtedy, ak spracúvanie spĺňa určité podmienky. Po prvé, zamestnávatelia, ktorí využívajú tieto produkty a aplikácie, musia posúdiť primeranosť opatrení, ktoré zavádzajú, a to, či sa môžu prijať ďalšie opatrenia na zmiernenie alebo zníženie rozsahu a dosahu spracúvania údajov. Príkladom osvedčeného postupu je, že by sa toto posúdenie mohlo uskutočniť prostredníctvom posúdenia vplyvu na ochranu údajov pred zavedením akejkoľvek monitorovacej technológie. Po druhé, zamestnávatelia musia zaviesť politiky prijateľného použitia popri politikách na ochranu súkromia a informovať o týchto

[17] Pozri vec *Halford/Spojené kráľovstvo*, [1997] ESĽP 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), v ktorej súd uviedol že, „telefonické hovory z prevádzkových priestorov, ako aj z domova, možno zahrnúť do pojmu „súkromný život“ a „korešpondencia“ v zmysle článku 8 odseku 1 [dohovoru]“; a vec *Barbulescu/Rumunsko*, [2016] ESĽP 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), ktorá sa týka používania profesijného účtu na odosielanie okamžitých správ na súkromnú korešpondenciu, v ktorej súd uviedol, že monitorovanie účtu zamestnávateľom bolo obmedzené a primerané; nesúhlasné stanovisko sudcu Pinta de Alberquerqua, ktorý argumentoval v prospech dosiahnutia dôslednej rovnováhy.

politikách, pričom opíšu prípustné použitie sietí a vybavenia organizácie a jednoznačne podrobne opíšu vykonávané spracúvanie.

V niektorých krajinách sa na vytvorenie takejto politiky zo zákona vyžaduje súhlas rady zamestnancov alebo podobného zastupiteľského orgánu zamestnancov. V praxi takéto politiky často navrhujú pracovníci údržby IT. Keďže ich hlavná pozornosť sa zameria hlavne na bezpečnosť a nie na oprávnené očakávania ochrany súkromia zamestnancov, pracovná skupina zriadená podľa článku 29 odporúča, aby sa vo všetkých prípadoch do posudzovania nevyhnutnosti monitorovania, ako aj logiky a prístupnosti politiky, zapojila reprezentatívna vzorka zamestnancov.

Príklad

Zamestnávateľ zavádza nástroj na ochranu pred únikom údajov na automatické monitorovanie odchádzajúcich e-mailov, a to na účely ochrany proti neoprávnenému prenosu informácií, ktoré sú predmetom priemyselného vlastníctva (napr. osobné údaje zákazníka), bez ohľadu na to, či je tento prenos neúmyselný. Keď sa e-mail považuje za potenciálny zdroj porušenia ochrany údajov, uskutoční sa ďalšie vyšetrovanie.

Zamestnávateľ sa opäť odvoláva na potrebu svojho oprávneného záujmu na ochranu osobných údajov zákazníkov, ako aj svojich aktív pred neoprávneným prístupom alebo únikom údajov. Takýto nástroj na ochranu pred únikom údajov sa môže týkať zbytočného spracúvania osobných údajov, napríklad upozornenie na „falošne pozitívny“ nález by mohlo viesť k neoprávnenému prístupu k legitímnym e-mailom, ktoré posielajú zamestnanci (ktorými môžu byť napríklad osobné e-maily).

Potreba nástroja na ochranu pred únikom údajov a jeho zavedenia by sa preto mala riadne odôvodniť, aby sa dosiahla správna rovnováha medzi oprávnenými záujmami zamestnávateľa a základným právom na ochranu osobných údajov zamestnancov. Na to, aby bolo možné uplatniť oprávnené záujmy zamestnávateľa, by sa mali prijať určité opatrenia na zmiernenie rizík. Napríklad pravidlá, ktorými sa systém riadi pri charakterizácii e-mailu ako možného porušenia ochrany údajov, by mali byť plne transparentné pre používateľov a v prípadoch, keď nástroj rozpozná e-mail pripravený na odoslanie ako potenciálne porušenie ochrany údajov, odosielateľa by mala informovať výstražná správa pred uskutočnením prenosu e-mailu, aby mal odosielateľ možnosť tento prenos zrušiť.

V určitých prípadoch je monitorovanie zamestnancov možné ani nie tak z dôvodu zavedenia konkrétnych technológií, ale jednoducho preto, lebo od zamestnancov sa očakáva, že budú používať online aplikácie poskytované zamestnávateľmi, ktoré spracúvajú osobné údaje. Príkladom je používanie cloudových kancelárskych aplikácií (napr. programy na úpravu dokumentov, kalendáre, sociálne siete). Malo by sa zabezpečiť, aby zamestnanci mohli určiť určité súkromné priestory, kam zamestnávateľ nemôže, až na mimoriadne okolnosti, získať prístup. Toto sa týka napríklad kalendárov, ktoré sa často používajú aj na plánovanie súkromných stretnutí. Ak zamestnanec plánované stretnutie označí ako „Súkromné“ alebo to uvedie v poznámke k samotnému stretnutiu, zamestnávateľovi (a ďalším zamestnancom) by sa nemalo povoliť skúmať obsah tohto stretnutia.

Požiadavka subsidiarity v tejto súvislosti občas znamená, že sa nesmie uskutočniť vôbec nijaké monitorovanie. To napríklad platí v prípade, keď zakázanému používaniu komunikačných služieb možno zabrániť zablokovaním určitých webových sídel. Ak je možné blokovať webové sídla namiesto neustáleho monitorovania všetkej komunikácie, na splnenie požiadavky subsidiarity by sa mala zvoliť možnosť blokovania webových sídel.

Vo všeobecnosti by sa prevencii mala dať oveľa väčšia váha než odhaľovaniu – záujmom zamestnávateľa lepšie poslúži predchádzanie zneužívaniu internetu prostredníctvom technických prostriedkov než vynakladaním zdrojov na jeho odhaľovanie.

5.4. Spracovateľské operácie vyplývajúce z monitorovania používania IKT mimo pracoviska

Používanie IKT mimo pracoviska sa stáva bežnejším s rastom možností práce z domu, práce na diaľku a zásadou „prines si vlastné zariadenie“. Schopnosti týchto technológií môžu

predstavovať riziko pre súkromný život zamestnancov, keďže v mnohých prípadoch monitorovacie systémy, ktoré existujú na pracovisku, sa v skutočnosti rozširujú do domácej sféry zamestnancov, ak takéto zariadenia používajú. .

5.4.1. *MONITOROVANIE PRÁCE Z DOMU A NA DIAĽKU*

Je čoraz častejšie, že zamestnávatelia ponúkajú zamestnancom možnosť pracovať na diaľku, napr. z domu a/alebo na ceste. V skutočnosti ide o hlavný faktor za zmenšením rozdielu medzi pracoviskom a domom. Vo všeobecnosti to znamená, že zamestnávateľ zamestnancom rozdá vybavenie IKT alebo softvér, ktoré im po nainštalovaní na ich zariadenia doma alebo na ich vlastné zariadenia umožňujú rovnakú úroveň prístupu do siete, systémov a zdrojov zamestnávateľa, aké by mali na pracovisku, a to v závislosti od realizácie.

Hoci práca na diaľku môže predstavovať pozitívny vývoj, takisto je oblasťou dodatočného rizika pre zamestnávateľa. Napríklad zamestnanci so vzdialeným prístupom do infraštruktúry zamestnávateľa, nie sú viazaní opatreniami týkajúcimi sa fyzickej bezpečnosti, ktoré môžu existovať v priestoroch zamestnávateľa. Jednoducho povedané: bez zavedenia vhodných technických opatrení sa zvyšuje riziko neoprávneného prístupu, čo môže viesť k strate alebo zničeniu informácií vrátane osobných údajov zamestnancov alebo zákazníkov, ktoré môže uchovávať zamestnávateľ.

Na zmiernenie tejto oblasti rizika sa zamestnávatelia môžu domnievať, že existuje dôvod na zavedenie softvérových balíkov (buď na mieste, alebo v rámci cloudu), ktoré majú schopnosť napríklad zaznamenávať stlačené klávesy alebo pohyby myši, zachytávať snímky obrazovky (buď náhodne, alebo v určených intervaloch), zaznamenávať používané aplikácie (a dĺžku ich používania) a na kompatibilných zariadeniach umožňujú používanie webových kamier a zber príslušných videozáznamov. Tieto technológie sú ľahko dostupné, a to aj od tretích strán, ako sú poskytovatelia cloudových služieb.

Spracúvanie údajov pomocou týchto technológií je však neprimerane veľké a je veľmi nepravdepodobné, že zamestnávateľ má právny dôvod v súlade s oprávneným záujmom, napr. zaznamenávať stlačenia klávesov alebo pohyby myši.

Zásadné je riešenie rizika, ktoré predstavuje práca z domu a práca na diaľku, primeraným a nie nadmerným spôsobom bez ohľadu na to, ako sa ponúka daná možnosť, a bez ohľadu na navrhovanú technológiu, najmä ak sú hranice medzi pracovným a súkromným použitím plynulé.

5.4.2. *PRINES SI VLASTNÉ ZARIADENIE (BRING YOUR OWN DEVICE – BYOD)*

Zamestnávatelia môžu z dôvodu nárastu obľúbenosti spotrebiteľských elektronických zariadení, ich charakteristík a schopností čeliť požiadavkám zamestnancov, aby na pracovisku mohli používať vlastné zariadenia na plnenie svojich pracovných povinností. Tento prístup je známy ako zásada „prines si vlastné zariadenie “.

Účinné vykonávanie tejto zásady môže mať pre zamestnancov niekoľko výhod vrátane vyššieho uspokojenia zamestnancov z práce, celkového zvýšenia pracovnej morálky, vyššej efektivity práce a väčšej flexibility. Z definície však vyplýva, že určité použitia zariadení zamestnancov budú svojou povahou osobné, a pravdepodobnosť súkromného použitia sa bude zvyšovať v určitom dennom čase (napr. večer alebo cez víkendy). Je preto nesporne možné, že používanie vlastných zariadení zamestnancov bude mať za následok, že

zamestnávatelia budú spracúvať informácie o týchto zamestnancoch a prípadne aj o rodinných príslušníkoch, ktorí tiež používajú dané zariadenia, pričom tieto informácie nesúvisia s podnikom.

V súvislosti so zamestnaním riziká pre súkromie vyplývajúce z prístupu „prines si vlastné zariadenie“ bežne súvisia s monitorovacími technológiami, ktoré zbierajú identifikačné údaje, ako sú MAC adresy, alebo s prípadmi, keď zamestnávateľ odôvodní prístup do zariadenia zamestnanca vykonaním bezpečnostnej kontroly, t. j. na nájdenie malvéru. Pokiaľ ide o bezpečnostné kontroly, existuje niekoľko komerčných riešení, ktoré umožňujú kontrolu súkromných zariadení, pri ich použití by však mohlo potenciálne dôjsť k prístupu k všetkým údajom na danom zariadení, a preto s nimi treba zaobchádzať s opatrnosťou. Napríklad prístup do častí zariadenia, o ktorých sa predpokladá, že sa používajú iba na súkromné účely (napr. priečinok, v ktorom sú uložené fotografie získané pomocou zariadenia), sa v podstate zakazuje.

Monitorovanie polohy a prevádzky týchto zariadení sa môže považovať za monitorovanie, ktoré slúži oprávnenému záujmu chrániť osobné údaje, za ktoré zamestnávateľ nesie ako prevádzkovateľ zodpovednosť. Toto monitorovanie však v prípade osobného zariadenia zamestnanca môže byť nezákonné, ak sa pri ňom zachytili aj údaje týkajúce sa súkromného a rodinného života zamestnanca. V záujme zabránenia tomu, aby sa monitorovali súkromné informácie, sa musia zaviesť vhodné opatrenia na rozlišovanie medzi súkromným a pracovným použitím zariadenia.

Zamestnávatelia by mali takisto zaviesť metódy, prostredníctvom ktorých sa ich vlastné údaje na zariadení môžu bezpečne prenášať medzi daným zariadením a ich sieťou. V niektorých prípadoch sa teda zariadenie nastaví tak, že sa všetka prevádzka presmeruje cez sieť VPN späť do podnikovej siete, čím sa zabezpečí určitá úroveň bezpečnosti. Ak sa však použije takéto opatrenie, zamestnávateľ by si mal uvedomiť, že softvér nainštalovaný na účely monitorovania predstavuje riziko pre ochranu súkromia v čase, keď zamestnanec zariadenie používa na osobné účely. Použiť by sa mohli zariadenia, ktoré ponúkajú dodatočnú ochranu, napríklad tzv. izolovanie (sandboxing) údajov (udržiavanie údajov v rámci osobitnej aplikácie).

A naopak, zamestnávateľ musí zvážiť aj zákaz používania konkrétnych pracovných zariadení na súkromné použitie, ak neexistuje spôsob, ako zabrániť monitorovaniu súkromného použitia – napríklad ak zariadenie ponúka vzdialený prístup k osobným údajom, v prípade ktorých zamestnávateľ plní úlohu prevádzkovateľa.

5.4.3. *SPRÁVA MOBILNÝCH ZARIADENÍ (MOBILE DEVICE MANAGEMENT – MDM)*

Zamestnávatelia prostredníctvom správy mobilných zariadení môžu na diaľku určovať polohu zariadení, zavádzať konkrétne nastavenia a/alebo aplikácie a na požiadanie vymazávať údaje. Zamestnávateľ môže túto funkciu obsluhovať sám alebo na to môže použiť tretiu stranu. Služby správy mobilných zariadení zamestnávateľom umožňujú aj vyhotovovať záznam zariadenia alebo ho sledovať v reálnom čase aj vtedy, keď nebola ohlásená jeho krádež.

Pred zavedením každej takejto technológie, ak ide o novú technológiu alebo o novú technológiu pre prevádzkovateľa, by sa malo uskutočniť posúdenie vplyvu na ochranu údajov. Ak výsledkom posúdenia vplyvu na ochranu údajov je, že technológia správy mobilných zariadení je za konkrétnych okolností potrebná, stále by sa malo uskutočniť

posúdenie o tom, či je výsledné spracúvanie údajov v súlade so zásadami proporcionality a subsidiarity. Zamestnávatelia musia zabezpečiť, že údaje zhromaždené v rámci tejto schopnosti zberu na diaľku sa budú spracúvať na určený účel a že netvoria a nemôžu tvoriť časť širšieho programu, ktorý umožňuje neustále monitorovanie zamestnancov. Aj v prípade určených účelov by sa prvky týkajúce sa sledovania mali zmierniť. Sledovacie systémy možno navrhnúť tak, že budú zaznamenávať lokalizačné údaje bez toho, aby sa poskytovali zamestnávateľovi. V takom prípade by sa lokalizačné údaje mali sprístupniť iba vtedy, keď sa ohlási krádež alebo strata zariadenia.

Zamestnancom, ktorých zariadenia patria do systému služieb správy mobilných zariadení, sa musia poskytnúť úplné informácie o tom, aké sledovanie prebieha a aké dôsledky pre nich z toho vyplývajú.

5.4.4. *NOSITEĽNÉ ZARIADENIA*

Zamestnávateľov čoraz viac láka, aby svojim zamestnancom poskytli nositeľné zariadenia na sledovanie a monitorovanie ich zdravotného stavu a činnosti na pracovisku a občas aj mimo neho. Takéto spracúvanie údajov sa však týka údajov o zdravotnom stave, a preto je na základe článku 8 smernice o ochrane údajov zakázané.

Vzhľadom na nerovnomerný vzťah medzi zamestnávateľmi a zamestnancami (t. j. zamestnanec je finančne závislý od zamestnávateľa) a so zreteľom na citlivosť údajov o zdravotnom stave je veľmi nepravdepodobné, aby bol poskytnutý právoplatný výslovný súhlas so sledovaním alebo monitorovaním týchto údajov, keďže v prvom rade zamestnanci v podstate nemôžu dať takýto súhlas „slobodne“. Spracúvanie bude nezákonné aj v prípade, ak zamestnávateľ na zber údajov o zdravotnom stave použije tretiu stranu, ktorá mu poskytne iba súhrn informácií o celkovom vývoji v oblasti zdravia.

Okrem toho, ako sa opisuje v *stanovisku č. 5/2014 k technikám anonymizácie*[18], je technicky veľmi náročné zabezpečiť úplnú anonymitu údajov. Ešte aj v prostredí, v ktorom je vyše tisíc zamestnancov, by zamestnávateľ vzhľadom na dostupnosť iných údajov o zamestnancoch stále mohol identifikovať jednotlivých zamestnancov s konkrétnymi zdravotnými ukazovateľmi, ako je vysoký krvný tlak alebo obezita.

Príklad:

Organizácia ponúkla svojim zamestnancom ako dar zariadenia na monitorovanie fyzickej zdatnosti. Zariadenia počítajú počet krokov, ktoré zamestnanci prejdú, a zaznamenávajú ich tep a spánkový vzorec.

K výsledným údajom o zdravotnom stave by mal mať prístup iba zamestnanec, a nie zamestnávateľ. Všetky údaje prenesené medzi zamestnancom (ako dotknutou osobou) a poskytovateľom zariadenia/služby (ako prevádzkovateľom) sa týkajú iba týchto strán.

Keďže zdravotné údaje môže spracúvať aj komerčná strana, ktorá zariadenia vyrobila alebo ktorá ponúka službu zamestnávateľom, zamestnávateľ by pri výbere zariadenia alebo služby mal vyhodnotiť politiku ochrany súkromia výrobcu a/alebo poskytovateľa služby, aby sa

[18] Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 5/2014 k technikám anonymizácie*, WP 216, 10. apríla 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

zabezpečilo, že použitím zariadenia alebo služby nedôjde k nezákonnému spracúvaniu zdravotných údajov zamestnancov.

5.5. Spracovateľské operácie súvisiace s časom a dochádzkou

Systémy, ktoré zamestnávateľom umožňujú kontrolovať, kto môže vstúpiť do priestorov ich prevádzky a/alebo do určitých oblastí v ich prevádzke, môžu umožňovať aj sledovanie činností zamestnancov. Hoci takéto systémy existujú už viacero rokov, čoraz viac sa zavádzajú nové technológie určené na sledovanie pracovného času a dochádzky zamestnancov vrátane technológií, ktoré spracúvajú biometrické údaje, ako aj iné technológie, napríklad na sledovanie mobilných zariadení.

Hoci tieto systémy môžu byť dôležitou súčasťou kontrolného záznamu zamestnávateľa, predstavujú aj riziko poskytnutia invazívnej úrovne poznatkov a kontroly, pokiaľ ide o činnosti zamestnancov na pracovisku.

Príklad:

Zamestnávateľ spravuje serverovú miestnosť, v ktorej sa v digitálnej podobe uchovávajú citlivé podnikové údaje, osobné údaje týkajúce sa zamestnancov a osobné údaje zákazníkov. Zamestnávateľ v záujme dodržania právnych záväzkov zabezpečiť údaje proti neoprávnenému prístupu inštaloval systém na kontrolu vstupu, ktorý zaznamenáva príchody a odchody zamestnancov s náležitým povolením vstupovať do miestnosti. Keby sa stratilo nejaké vybavenie alebo keby došlo k neoprávnenému prístupu k údajom, ich strate alebo krádeži, záznamy, ktoré zamestnávateľ uchováva mu umožnia určiť, kto do miestnosti vstúpil v danom čase.

Vzhľadom na to, že spracúvanie je nevyhnutné a neprevažuje nad právom zamestnancov na súkromný život, môže ísť o oprávnený záujem podľa článku 7 písm. f), pokiaľ boli zamestnanci o spracovateľskej operácii náležite informovaní. Neustále monitorovanie periodicity a presných časov príchodu a odchodu zamestnancov však nemôže byť oprávnené, ak sa tieto údaje používajú aj na iný účel, ako je hodnotenie výkonu zamestnancov.

5.6. Spracovateľské operácie využívajú videomonitorovacie systémy

Monitorovanie kamerovým systémom stále predstavuje podobné problémy, pokiaľ ide o súkromie zamestnancov, ako v minulosti: schopnosť nepretržite zaznamenávať správanie pracovníka[19]. Najvýznamnejšími zmenami týkajúcimi sa používania tejto technológie v súvislosti so zamestnaním je schopnosť ľahkého prístupu k zhromaždeným údajom na diaľku (napr. prostredníctvom smartfónu); zmenšenie rozmeru kamier (spoločne so zvýšením ich schopností, napr. vysoké rozlíšenie); a spracúvanie, ktoré sa môže uskutočniť prostredníctvom nových metód analýzy videozáznamov.

So schopnosťami poskytovanými nástrojmi na analýzu videozáznamov môže zamestnávateľ automatickými prostriedkami monitorovať výrazy tváre pracovníka s cieľom zistiť odchýlky od vopred vymedzených pohybov (napr. továrenský kontext) a ešte viac. Toto použitie by nebolo primerané k právam a slobodám zamestnancov, a preto by bolo vo všeobecnosti

[19] Pozri uvedený rozsudok vo veci *Köpke/Nemecko*; navyše treba poznamenať aj to, že v niektorých jurisdikciách súdy rozhodli o prípustnosti inštalovania systémov, ako je priemyselná televízia, na účely preukazovania nezákonného správania; pozri vec *Bershka* pred španielskym ústavným súdom.

nezákonné. Súčasťou spracúvania môže byť aj profilovanie a prípadne automatizované rozhodovanie. Zamestnávatelia by sa teda mali vyhýbať používaniu technológií na rozpoznávanie tváre. Toto pravidlo môže mať určité okrajové výnimky, takéto scenáre sa však nemôžu použiť na uplatnenie všeobecného uznania používania takejto technológie[20].

5.7. Spracovateľské operácie týkajúce sa vozidiel používaných zamestnancami

Technológie, ktoré zamestnávateľom umožňujú monitorovať ich vozidlá, sa značne rozšírili, najmä medzi organizáciami, ktorých činnosti súvisia s dopravou alebo ktoré majú veľké vozové parky.

Každý zamestnávateľ, ktorý používa vozidlovú telematiku, zbiera údaje o vozidle a o konkrétnom zamestnancovi, ktorý dané vozidlo používa. Súčasťou týchto údajov nemusí byť iba poloha vozidla (a teda aj zamestnanca) získaná pomocou systémov základného sledovania polohy pomocou GPS, ale v závislosti od technológie aj množstvo ďalších informácií vrátane informácií o správaní pri vedení vozidla. Určité technológie môžu umožňovať aj súvislé monitorovanie vozidla aj vodiča (napr. prístroje na záznam údajov o udalostiach).

Zamestnávateľ by mohol mať povinnosť inštalovať do vozidiel sledovaciu techniku s cieľom preukázať súlad s inými právnymi záväzkami, napr. s cieľom zaručiť bezpečnosť zamestnancov, ktorí riadia dané vozidlá. Zamestnávateľ môže mať aj oprávnený záujem, aby mohol kedykoľvek určiť polohu svojich vozidiel. Aj keby zamestnávatelia mali oprávnený záujem dosiahnuť splnenie týchto účelov, malo by sa najprv posúdiť, či je spracúvanie na tieto účely potrebné a či je samotná realizácia v súlade so zásadami proporcionality a subsidiarity. Ak je možné používať služobné vozidlo na súkromné účely, najdôležitejším opatrením, ktoré zamestnávateľ môže prijať na zabezpečenie súladu s týmito zásadami, je ponuka výnimky: v zásade by zamestnanec mal mať možnosť dočasne vypnúť sledovanie polohy, pokiaľ to odôvodňujú osobitné okolnosti, ako je návšteva u lekára. Týmto spôsobom môže zamestnanec vlastnou iniciatívou chrániť určité lokalizačné údaje ako súkromné. Zamestnávateľ musí zabezpečiť, aby sa získané údaje nepoužívali na nezákonné ďalšie spracúvanie, ako je sledovanie a hodnotenie zamestnancov.

Zamestnávateľ takisto musí jednoznačne informovať zamestnancov o tom, že v podnikovom vozidle, ktoré riadia, je inštalované sledovacie zariadenie a že ich pohyb počas používania daného vozidla sa zaznamenáva (a že v závislosti od príslušnej technológie sa môže zaznamenávať aj ich správanie pri vedení vozidla). Tieto informácie by sa, pokiaľ možno, mali viditeľne zobrazovať v každom vozidle, a to na mieste viditeľnom z miesta vodiča.

Je možné, že zamestnanci môžu podnikové vozidlá používať mimo pracovných hodín, napr. na osobné účely, v závislosti od konkrétnych politík, ktorými sa riadi použitie týchto vozidiel. Vzhľadom na citlivosť lokalizačných údajov je nepravdepodobné, že existuje právny základ na monitorovanie polohy vozidiel zamestnancov mimo dohodnutých pracovných hodín. Ak by však existovala takáto potreba, malo by sa zvážiť zavedenie, ktoré bude primerané rizikám. To by napríklad mohlo znamenať, že na zabránenie krádeže vozidla sa mimo pracovných hodín nezaznamená poloha automobilu, pokiaľ vozidlo neopustí určitý široko vymedzený okruh (región či dokonca krajinu). Navyše sa poloha zobrazí iba v prípade

[20] Okrem toho sa spracúvanie biometrických údajov na účely identifikácie podľa všeobecného nariadenia o ochrane údajov musí zakladať na výnimke uvedenej v článku 9 ods. 2.

krádeže – zamestnávateľ aktivuje „viditeľnosť“ polohy iba vtedy, keď vozidlo opustí vymedzený región, čím sa dostane k údajom, ktoré už systém uložil.

Ako uvádza pracovná skupina zriadená podľa článku 29 v *stanovisku č. 13/2011 ku geolokačným službám v inteligentných mobilných zariadeniach*[21]:

„Zariadenia na sledovanie vozidiel nie sú zariadeniami na sledovanie zamestnancov. Ich funkcia spočíva v sledovaní alebo monitorovaní polohy vozidiel, v ktorých sú inštalované. Zamestnávatelia by ich nemali považovať za zariadenia na sledovanie alebo monitorovanie správania alebo miesta pobytu vodičov alebo iných zamestnancov, napríklad vysielaním výstrah v súvislosti s rýchlosťou vozidla.“

Navyše ako sa uvádza v *stanovisku č. 5/2005 pracovnej skupiny zriadenej podľa článku 29 k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou*[22]:

„Spracúvanie miestnych údajov musí byť odôvodnené v prípadoch, keď sa vykonáva ako súčasť sledovania dopravy ľudí alebo tovarov, alebo zlepšovania rozdeľovania zdrojov pri službách v izolovaných oblastiach (napr. plánovanie činností v reálnom čase) alebo keď je cieľom bezpečnosť samotného zamestnanca, tovarov alebo vozidiel, ktoré má na starosti. Pracovná skupina naopak považuje spracúvanie údajov za prehnané v prípadoch, keď si zamestnanci môžu slobodne a podľa želania organizovať svoje cesty, alebo keď jeho jediným účelom je sledovať prácu zamestnanca, ktorá sa dá sledovať aj inými spôsobmi.“

5.7.1. PRÍSTROJE NA ZÁZNAM ÚDAJOV O UDALOSTIACH

Prístroje na záznam údajov o udalostiach poskytujú zamestnávateľovi technickú schopnosť spracúvať značné množstvo osobných údajov o zamestnancoch, ktorí riadia podnikové vozidlá. Takéto zariadenia sa čoraz častejšie umiestňujú do vozidiel s cieľom vytvárať videozáznam, ktorý prípadne obsahuje aj zvuk, a to pre prípad nehody. Tieto systémy dokážu zaznamenávať v určitom čase, napr. v reakcii na náhle brzdenie, neočakávanú zmenu smeru alebo nehody, pri ktorých sa uchovajú okamihy bezprostredne predchádzajúce nehode, je však možné ich nastaviť aj na neustále monitorovanie. Tieto informácie možno neskôr použiť na pozorovanie a preskúmanie správania jednotlivca pri vedení vozidla s cieľom toto správanie zlepšiť. Veľa z týchto systémov okrem toho obsahuje systém GPS na sledovanie polohy vozidla v reálnom čase a na ďalšie spracúvanie možno uložiť aj iné podrobnosti týkajúce sa riadenia (napríklad rýchlosť vozidla).

Tieto zariadenia sa obzvlášť rozšírili medzi organizáciami, ktorých činnosti súvisia s dopravou alebo ktoré majú veľké vozidlové parky. Zavedenie prístrojov na záznam údajov o udalostiach však môže byť zákonné iba vtedy, ak existuje potreba spracúvať výsledné osobné údaje týkajúce sa zamestnanca na legitímny účel a ak je spracúvanie v súlade so zásadami proporcionality a subsidiarity.

Príklad

[21] Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 13/2011 ku geolokačným službám v inteligentných mobilných zariadeniach*, WP 185, 16. mája 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[22] Pracovná skupina zriadená podľa článku 29, *Stanovisko č. 5/2005 k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou*, WP 115, 25. novembra 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf.

Prepravná spoločnosť vybaví všetky svoje vozidlá palubnou videokamerou, ktorá zaznamenáva zvuk a obraz. Účelom spracúvania týchto údajov je zlepšenie vodičských zručností zamestnancov. Kamery sú nastavené tak, aby uchovávali záznamy vždy, keď vodič náhle zabrzdí alebo keď neočakávane zmení smer. Spoločnosť predpokladá, že jej právnym dôvodom na spracúvanie je oprávnený záujem podľa článku 7 písm. f) smernice chrániť bezpečnosť zamestnancov a ďalších vodičov.

Oprávnený záujem spoločnosti monitorovať vodičov však neprevažuje nad právami týchto vodičov na ochranu ich osobných údajov. Neustále monitorovanie zamestnancov pomocou takýchto kamier predstavuje závažný zásah do ich práva na súkromie. Existujú iné metódy (napr. inštalácia vybavenia, ktoré bráni používaniu mobilných telefónov), ako aj iné bezpečnostné systémy, ako sú zdokonalené systémy núdzového brzdenia a systémy výstrahy pred vybočením z jazdného pruhu, ktoré možno použiť na predchádzanie automobilovým nehodám a ktoré by mohli byť vhodnejšie. Okrem toho je veľmi pravdepodobné, že takéto video povedie k spracúvaniu osobných údajov tretích strán (ako sú chodci), a v prípade tohto spracúvania oprávnený záujem spoločnosti nestačí na jeho odôvodnenie.

5.8. Spracovateľské operácie týkajúce sa poskytnutia údajov o zamestnancovi tretím stranám

Čoraz častejšie spoločnosti prenášajú údaje svojich zamestnancov svojim zákazníkom na účely zabezpečenia spoľahlivého poskytovania služieb. Tieto údaje môžu byť celkom nadbytočné, a to v závislosti od rozsahu poskytovaných služieb (napr. možno uviesť fotografiu zamestnanca). Zamestnanci však vzhľadom na nerovnováhu moci nemôžu dať slobodný súhlas so spracúvaním svojich osobných údajov zo strany zamestnávateľa, a ak spracúvanie údajov nie je primerané, zamestnávateľ nemá právny dôvod.

Príklad:

Doručovacia spoločnosť posiela svojim zákazníkom e-mail s odkazom na meno a polohu doručovateľa (zamestnanca). Spoločnosť takisto zamýšľala poskytnúť pasovú fotografiu doručovateľa. Spoločnosť predpokladala, že jej právny dôvod na spracúvanie spočíva v oprávnenom záujme [článok 7 písm. f) smernice] umožniť zákazníkovi overiť, či je doručovateľ skutočne správnou osobou.

Poskytnutie mena a fotografie doručovateľa zákazníkom však nie je nevyhnutné. Keďže neexistuje nijaký iný oprávnený dôvod na toto spracúvanie, doručovacia spoločnosť nesmie zákazníkom poskytnúť tieto osobné údaje.

5.9. Spracovateľské operácie týkajúce sa medzinárodných prenosov údajov v oblasti ľudských zdrojov a iných zamestnaneckých údajov

Zamestnávatelia čoraz častejšie používajú cloudové aplikácie a služby, ako sú aplikácie a služby určené na správu údajov v oblasti ľudských zdrojov, ako aj online kancelárske aplikácie. Výsledkom používania väčšiny týchto aplikácií bude medzinárodný prenos údajov od zamestnancov, ktoré sa ich týkajú. Ako sa opisovalo už v stanovisku č. 8/2001, v článku 25 smernice sa uvádza, že prenosy osobných údajov do tretej krajiny mimo EÚ sa môžu uskutočňovať iba vtedy, keď daná krajina zabezpečí adekvátnu úroveň ochrany. Bez ohľadu na základ, prenos by mal vyhovovať ustanoveniam smernice.

Malo by sa teda zabezpečiť dodržanie týchto ustanovení týkajúcich sa medzinárodného prenosu údajov. Pracovná skupina zriadená podľa článku 29 opakovane uvádza svoju predchádzajúcu pozíciu, že vhodnejšie je uplatňovať primeranú ochranu namiesto odchýlok uvedených v článku 26 smernice o ochrane údajov; ak sa uplatňuje súhlas, musí byť tento súhlas konkrétny, jednoznačný a vydaný slobodne. Malo by sa však takisto zabezpečiť, že údaje poskytované mimo krajín EÚ/EHP a neskorší prístup iných subjektov v rámci skupiny ostanú obmedzené na minimum nevyhnutné na plánované účely.

6. Závery a odporúčania

6.1. Základné práva

Na obsah uvedenej komunikácie, ako aj na prevádzkové údaje súvisiace s touto komunikáciou, sa vzťahuje rovnaká ochrana základných práv ako na „analógovú“ komunikáciu.

Elektronickú komunikáciu z prevádzkových priestorov možno zahrnúť do pojmov „súkromný život“ a „korešpondencia“ v zmysle článku 8 odseku 1 európskeho dohovoru. Zamestnávatelia na základe súčasnej smernice o ochrane údajov môžu zbierať údaje iba na legitímne účely, pričom spracúvanie sa uskutočňuje za vhodných podmienok (napr. musí byť primerané a nevyhnutné, na účely skutočného a prítomného záujmu, zákonným, pevne stanoveným a transparentným spôsobom) s právnym základom na spracúvanie osobných údajov zhromaždených alebo získaných prostredníctvom elektronickej komunikácie.

Skutočnosť, že zamestnávateľ vlastní elektronické prostriedky, nevylučuje právo zamestnancov na dôvernosť ich komunikácie, súvisiace lokalizačné údaje a listové tajomstvo. Sledovanie polohy zamestnancov prostredníctvom ich vlastných alebo podnikových zariadení by sa malo obmedziť na situácie, v ktorých je jednoznačne nevyhnutné na legitímny účel. Samozrejme, v prípade zásady „prines si vlastné zariadenie“ je dôležité, aby zamestnanci mali príležitosť ochrániť svoju súkromnú komunikáciu pred akýmkoľvek monitorovaním súvisiacim s prácou.

6.2. Súhlas; oprávnený záujem

Zamestnanci takmer nikdy nie sú v postavení, v ktorom by mohli slobodne udeliť, zamietnuť alebo zrušiť súhlas vzhľadom na závislosť vyplývajúcu zo vzťahu medzi zamestnávateľom a zamestnancom. Zamestnanci môžu vzhľadom na nerovnováhu moci dať slobodný súhlas iba za mimoriadnych okolností, keď s prijatím alebo zamietnutím ponuky nie sú spojené vôbec nijaké následky.

Oprávnený záujem zamestnávateľov sa občas môže uplatniť ako právny dôvod, ale iba vtedy, ak je spracúvanie jednoznačne potrebné na legitímny účel a ak je v súlade so zásadami proporcionality a subsidiarity. Pred zavedením akéhokoľvek monitorovacieho nástroja by sa mal uskutočniť test proporcionality s cieľom posúdiť, že sú všetky údaje nevyhnutné, či toto spracúvanie prevažuje všeobecné práva na súkromie, ktoré zamestnanci majú aj na pracovisku, a s cieľom posúdiť, aké opatrenia sa musia prijať, aby sa zabezpečilo, že porušovanie práva na súkromný život a práva na dôvernosť komunikácie sa obmedzí na nevyhnutné minimum.

6.3. Transparentnosť

So zamestnancami by sa mala viesť efektívna komunikácia týkajúca sa každého vykonávaného monitorovania, účelov tohto monitorovania a okolností, ako aj možností zamestnancov, ako môže zabrániť zhromažďovaniu ich údajov monitorovacími technológiami. Politiky a pravidlá týkajúce sa oprávneného monitorovania musia byť zrozumiteľné a rýchlo dostupné. Pracovná skupina odporúča, aby sa do vytvorenia a hodnotenia týchto pravidiel a politík zapojila reprezentatívna vzorka zamestnancov, keďže väčšina monitorovania má potenciál narúšať súkromné životy zamestnancov.

6.4. Proporcionalita a minimalizácia údajov

Spracúvanie údajov v práci musí byť primeranou reakciou na riziká, ktorým čelí zamestnávateľ. Napríklad zneužívanie internetu možno odhaliť bez potreby analyzovať obsah webových sídel. Ak je zneužívaniu možné zabrániť (napr. používaním webových filtrov), zamestnávateľ nemá nijaké všeobecné právo monitorovať zamestnanca.

Okrem toho úplný zákaz komunikácie z osobných dôvodov je nepraktický a jeho presadzovanie si môže vyžadovať takú úroveň monitorovania, ktorá by mohla byť neprimeraná. Prevencii by sa mala dať oveľa väčšia váha než odhaľovaniu – záujmom zamestnávateľa lepšie poslúži predchádzanie zneužívaniu internetu prostredníctvom technických prostriedkov než vynakladaním zdrojov na jeho odhaľovanie.

Informácie zaznamenané z prebiehajúceho monitorovania, ako aj informácie, ktoré sa ukazujú zamestnávateľovi, by sa mali čo najviac minimalizovať. Zamestnanci by mali mať možnosť dočasne vypnúť sledovanie polohy, ak to je odôvodnené okolnosťami. Riešenia, ktoré napríklad sledujú vozidlá, sa môžu navrhnúť tak, aby zaznamenávali údaje o polohe bez toho, aby sa predkladali zamestnávateľovi.

Zamestnávatelia musia pri rozhodovaní o zavedení nových technológií zohľadniť zásadu minimalizácie údajov. Informácie by sa mali uchovávať počas minimálne potrebného obdobia, pričom sa stanoví obdobie uchovávania údajov. Vždy, keď už informácie nie sú potrebné, mali by sa vymazať.

6.5. Služby cloudu, online aplikácie a medzinárodné prenosy

Keď sa od zamestnancov očakáva, že budú používať online aplikácie, ktoré spracúvajú osobné údaje (napríklad online kancelárske aplikácie), zamestnávatelia by mali zvážiť, že zamestnancom umožnia určiť určité súkromné priestory, kam zamestnávateľ nemôže, až na mimoriadne okolnosti, získať prístup, ako je priečinok so súkromnou poštou alebo dokumentmi.

Používanie väčšiny aplikácií v cloude má za následok medzinárodný prenos údajov zamestnancov. Malo by sa zabezpečiť, že prenos osobných údajov do tretej krajiny mimo EÚ sa bude uskutočňovať iba vtedy, ak sa zabezpečí adekvátna úroveň ochrany, a že údaje poskytované mimo krajín EÚ/EHP a neskorší prístup iných subjektov v rámci skupiny ostanú obmedzené na minimum nevyhnutné na plánované účely.

* * *

V Bruseli 8. júna 2017

Za pracovnú skupinu

predsedníčka
Isabelle FALQUE-PIERROTIN