

G

D

P

R

A OCHRANA ZÁUJMOV
ZAMESTNANCA

Marek Švec

Jana Žulová

Jana Žuřová - Marek Švec

**GDPR
a ochrana záujmů
zaměstnanca**

BRATISLAVA 2018

Autorský kolektív

© JUDr. Jana Žulová, PhD.

© doc. JUDr. Marek Švec, PhD., LL.M.

Recenzenti

doc. JUDr. Mgr. Andrea Olšovská, PhD.

JUDr. Marcel Dolobáč, PhD.

JUDr. Simona Schuszteková, PhD., LL.M.

Vedecká monografia vznikla ako výstup medzinárodného projektu Friedrich Ebert Stiftung, zastúpenie v Slovenskej republike pod názvom “*Kultúra sveta práce/Kultur der Arbeitswelt*”

Právne výklady a stanoviská obsiahnuté v texte publikácie sú subjektívnym názorom autorského kolektívu, nemožno ich stotožňovať s postojmi Friedrich Ebert Stiftung, e.V. alebo Labour Law Association/Asociácia pracovného práva.

Toto dielo a ani žiadnu jeho časť nemožno reprodukovat' bez súhlasu Friedrich Ebert Stiftung, e.V.

Vydavateľ: Friedrich Ebert Stiftung, zastúpenie v Slovenskej republike; Bratislava 2018

Návrh obálky: Mgr. Jakub Filo

Rok a miesto vydania: Bratislava, 2018

Rozsah publikácie: 10,4 AH

ISBN 978–80–89149–57–5 (tlačený - lepený/mäkká väzba)

Obsah

ZOZNAM AUTOROV	6
Úvod	10
I. Právne základy ochrany súkromia zamestnanca a ochrany osobných údajov	11
1.1 Všeobecný právny rámec	11
1.2 Právna úprava v oblasti občianskeho a pracovného práva	17
1.3 Právna úprava v oblasti ochrany osobných údajov – všeobecné nariadenie o ochrane údajov	20
1.3.1 Nový legislatívny rámec pri ochrane osobných údajov	21
II. Pôsobnosť GDPR a nového zákona o ochrane osobných údajov	24
2.1. Územná pôsobnosť	24
2.2. Vecná pôsobnosť	26
2.2.1. Všeobecné osobné údaje	26
2.2.2. Osobitná kategória osobných údajov (tzv. citlivé údaje)	28
2.2.3. Všeobecné osobné údaje a citlivé osobné údaje zamestnanca	29
2.3. Kľúčové zásady spracúvania osobných údajov	30
2.3.1 Zásada obmedzenia účelu a zásada minimalizácie údajov	30
2.3.2 Zákonnosť spracúvania	33
2.3.2.1 Druhy právnych základov pri spracúvaní všeobecných osobných údajov	34
2.3.2.2 Druhy právnych základov pri spracúvaní citlivých osobných údajov	41
III. Zamestnanec v pozícii dotknutej osoby	44
3.1 Dotknutá osoba	44
3.2 Právna subjektivita dotknutej osoby	45
3.3. Práva dotknutej osoby	46
3.3.1. Právo na informácie	47
3.3.2 Právo na prístup	55
3.3.3 Právo na opravu	56
3.3.4 Právo na vymazanie (právo „na zabudnutie“)	57
3.3.5 Právo na obmedzenie spracúvania	59
3.3.6 Právo na prenosnosť osobných údajov	60

3.3.7 Právo namietat'	63
3.3.8 Právo na neúčinnosť automatizovaného individuálneho rozhodovania, vrátane profilovania	64
3.3.9. Povinnosti prevádzkovateľa (zamestnávateľa) pri uplatňovaní práv dotknutej osoby	68

IV. Spracúvanie osobných údajov v individuálnych pracovnoprávných vzťahoch (praktické prípady)

4.1 Vyhľadávanie zamestnancov cez sociálne siete	73
4.2 Spracúvanie osobných údajov v životopisoch a vytváranie databázy životopisov	77
4.3 Pracovný pohovor z pohľadu ochrany osobných údajov	80
4.4 Zisťovanie zdravotnej a psychickej spôsobilosti uchádzačov o zamestnanie	83
4.5 Uvádzanie rodného čísla v pracovnej zmluve	89
4.6 Kopírovanie a skenovanie úradných dokladov zamestnancov	92
4.7 Vedenie osobného (personálneho) spisu zamestnanca	94
4.8 Fotografia zamestnanca a zverejňovanie ďalších osobných údajov zamestnanca	95
4.9 Evidencia dochádzky a vstup do priestorov založený na biometrickom údají	99
4.10 Monitorovanie komunikačných prostriedkov na pracovisku	102
4.11. Monitorovanie priestorov a zamestnancov kamerovými systémami	107
4.12 Whistleblowing	110

V. Spracúvanie osobných údajov v kolektívnych pracovnoprávných vzťahoch (praktické prípady)

5.1 Spracúvanie informácie o členstve zamestnanca v odboroch odborovou organizáciou - uplatnenie výnimky v zmysle čl. 9 ods. 2 písm. d) nariadenia	112
5.2 Spracúvanie informácie o členstve zamestnanca v odboroch odborovou organizáciou - súhlas zamestnanca čl. 9 ods. 2 písm. a) nariadenia	118
5.3 Spracúvanie osobných údajov odborovo organizovaného a odborovo neorganizovaného zamestnanca odborovou organizáciou	120

5.4	Realizácia zrážok zo mzdy a spracúvanie informácie o členstve zamestnanca v odborovej organizácii zamestnávateľom	123
5.5	Možnosti zvýšenia pracovnoprávnej ochrany zamestnancov prostredníctvom kolektívnej zmluvy	126
Záver		129
Zoznam použitej literatúry		130

ZOZNAM AUTOROV

JUDr. Jana Žulová, PhD.

Jana Žulová vyštudovala právo na Právnickej fakulte Univerzity Pavla Jozefa Šafárika v Košiciach a od roku 2010 pôsobí na tunajšej Katedre pracovného práva a práva sociálneho zabezpečenia. Je členkou Labour Law Association/Asociácie pracovného práva, ktorá spája odborníkov z oblasti pracovného práva a príbuzných odborov. Je autorkou a spoluautorkou viacerých vedeckých i odborných článkov z odboru, prednáša primárne problematiku pracovného práva a poskytuje právne poradenstvo a konzultantské služby týkajúce sa pracovnoprávnych vzťahov, s presahom aj do oblasti ľudských zdrojov. V rámci svojej vedeckej profilácie sa orientuje na problematiku harmonizácie rodinnej a pracovnej sféry a skúmania pracovných podmienok vybraných skupín zamestnancov (mladiství, absolventi, zamestnanci so zdravotným postihnutím, osoby 55+), čo dokumentuje viac ako 40 publikácií vedeckého charakteru. Za posledné štyri roky sa aktívne zúčastnila úspešne ukončeného riešenia dvoch projektov VEGA (VEGA č. 1/0851/12, VEGA č. 1/0805/13) a troch štrukturálnych projektov (IRES – tvorca IT nástroja pre pracovné právo, RIFIV – vytvorenie interdisciplinárnych predmetov pre zlepšenie uplatnenia absolventov na trhu práce a Učíme sa celý život – tvorba vzdelávacieho programu podporujúceho aktívne starnutie). V súčasnosti je spoluriešiteľkou dvoch vedeckých projektov APVV.

doc. JUDr. Marek Švec, PhD., LL.M.

Marek Švec je generálnym tajomníkom a súčasne členom Predsedníctva Labour Law Association/Asociácia pracovného práva. Vyštudoval Právnickú fakultu Trnavskej univerzity v Trnave, je absolventom doktorandského štúdia na Právnickej fakulte Trnavskej univerzity v Trnave, ako aj postgraduálneho štúdia Business Legal Relations na International School of Management. V roku 2017 úspešne absolvoval habilitačné konanie na Právnickej fakulte Trnavskej univerzity v Trnave a bol mu udelený vedecko-pedagogický titul „*docent*“ v študijnom odbore Pracovné právo. V minulosti pôsobil ako podpredseda poradnej komisie ministra práce, sociálnych vecí a rodiny SR pre rozširovanie záväznosti kolektívnych zmlúv vyššieho stupňa a člen tripartitnej komisie pre prípravu novely zákona o kolektívnom vyjednávaní, pričom sa podieľal aj na príprave ďalších noviel pracovnoprávnych predpisov (napr. Zákonníka práce). V súčasnosti pôsobí ako právny poradca Moderných odborov Volkswagen, odborového zväzu Moderné odbory AIOS a poskytuje právne poradenstvo pre zamestnávateľské organizácie z rôznych hospodárskych sektorov. Rovnako je pedagogicky činný a pôsobí na Katedre právnych a humanitných vied FMK UCM. Je vedený ako sprostredkovateľ a rozhodca kolektívneho vyjednávania v zozname Ministerstva práce, sociálnych vecí a rodiny

SR na roky 2016 – 2018. Popri profesijnej činnosti je publikačne aktívny. Je autorom a spoluautorom domácich a zahraničných monografických diel, vedeckých prác a článkov z oblasti pracovného práva, publikovaných v domácich i zahraničných periodikách a konferenčných zborníkoch, vrátane výstupov evidovaných vo svetových databázach.

POUŽITÉ SKRATKY PRÁVNÝCH PREDPISOV

GDPR Nariadenie Európskeho parlamentu a Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica č. 95/46/ES (všeobecné nariadenie o ochrane údajov)

nový zákon o OOÚ

zákon v legislatívnom procese pod číslom LP/2017/453, ktorým sa ruší zákon č. 122/2013 Z. z. o ochrane osobných údajov v znení neskorších predpisov (stav k 31. októbru 2017)

starý zákon o OOÚ

zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Občiansky zákonník, OZ

zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov

Obchodný zákonník, OBZ

zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

Ústava SR

ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky

zákon o archívoch a registratúrach

zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov

zákon o bezpečnosti a ochrane zdravia pri práci

zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

zákon o dani z príjmov

zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov

zákon o ochrane verejného zdravia

zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

zákon o slobode informácií

zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

zákon o sociálnom фонде

zákon č. 152/1994 Z. z. o sociálnom фонде a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov

zákon o sociálnom poistení

zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov

zákon o účtovníctve

zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov

zákon o zdravotnom poistení

zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

zákon o združovaní občanov

zákon č. 83/1990 Zb. o združovaní občanov v znení neskorších predpisov

Zákonník práce, ZP

zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov

POUŽITÉ SKRATKY A ZNAČKY

BOZP – bezpečnosť a ochrana zdravia na pracovisku

EÚ – Európska únia

MOP – Medzinárodná organizácia práce

pracovná skupina WP 29 – pracovná skupina pre ochranu údajov zriadená podľa článku 29 Smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov

SD EÚ – Súdny dvor Európskej únie

ust. – ustanovenie

Úrad – Úrad na ochranu osobných údajov Slovenskej republiky

ÚS SR – Ústavný súd Slovenskej republiky

Úvod

Nový právny rámec ochrany osobných údajov, tvorený európskym všeobecným nariadením o ochrane údajov a novým slovenským zákonom o ochrane osobných údajov, predstavuje pre mnoho dotknutých osôb, ktoré by sa ním mali riadiť, nanešťastie ešte stále pomerne veľkú neznámu. K tejto skutočnosti neprispieva len ľudská vlastnosť nechávať si vybavovanie náročných vecí na poslednú chvíľu, kedy sa už tomu nedá vyhnúť, ale objektívne celú situáciu nedostatočného povedomia o nových právach, alebo povinnostiach dotknutých subjektov komplikuje i v zásade neexistencia žiadnej relevantnej odbornej literatúry, ktorá by dokázala primeraným spôsobom objasniť postup subjektov v novom právnom stave. O to náročnejšie je preto potrebné vnímať aktuálne problémy zamestnávateľov i zamestnancov, ktorých sa nový právny rámec dotýka výrazne bezprostrednejšie ako subjektov v iných hospodárskych odvetviach, resp. subjektov v právnom postavení, napr. samostatne zárobkovo činných osôb.

V nadväznosti na opakované požiadavky i dotazy z aplikačnej praxe sme sa preto rozhodli, aj s ohľadom na vlastné profesionálne zameranie i predchádzajúce teoretické i praktické skúsenosti s ochranou osobných údajov, v súčasnom právnom rámci pripraviť predkladanú publikáciu dotýkajúcu sa identifikácie zmien, ktoré si vyžiada pri realizácii pracovnoprávných vzťahov predovšetkým uplatnenie nového všeobecného nariadenia o ochrane osobných údajov.

Postupným predmetom výkladu sa stáva nielen otázka práva na súkromie, ako základného imperatívu ochrany osobných údajov, ale aj otázky súvisiace vôbec s vymedzením okruhu dotknutých subjektov, konkretizácie ich práv a povinností alebo upresnenia nových právnych inštitútov, ktoré so sebou nová legislatíva prináša. Základnou pridanou hodnotou publikácie je však pomerne rozsiahla kapitola, ktorá prostredníctvom jednotlivých prípadových štúdií umožňuje čitateľovi osvojiť si náročnú problematiku v osobitostiach a ilustráciách na konkrétnych otázkach, s ktorými sa vo svojej praxi stretáva najčastejšie. Výber prípadových štúdií bol ovplyvnený predovšetkým najčastejšími aplikačnými problémami, s ktorými sa zamestnávatelia alebo zamestnanci stretávajú pri realizácii pracovnoprávných vzťahov.

V neposlednom rade by sme sa chceli poďakovať Friedrich Ebert Stiftung, zastúpenie v SR, keďže predmetná publikácia vznikla v rámci projektu *“Kultúra sveta práce/ Kultur der Arbeitswelt”*, čím sa umožní sprístupniť ju širokému diapazónu dotknutých osôb, ktorých sa problematika nového právneho rámca ochrany osobných údajov dotýka.

I. Právne základy ochrany súkromia zamestnanca a ochrany osobných údajov

1.1 Všeobecný právny rámec

Všeobecný právny rámec v oblasti ochrany práva na súkromný a rodinný život (a ochrany osobných údajov, ako jeho integrálnej súčasti) v rámci pracovnoprávných vzťahov predstavuje medzinárodná a európska právna úprava a na národnej úrovni Ústava SR.¹ Osobitnú právnu úpravu na národnej úrovni budú následne tvoriť okrem iného aj Zákonník práce, Občiansky zákonník, pripravovaný zákon o ochrane osobných údajov, ktorý transponuje všeobecné nariadenie o ochrane osobných údajov do slovenského právneho poriadku.

Pred neskôr uvádzaným právnym výkladom, snažiacim sa o vymedzenia práva na súkromie, je nevyhnutné uviesť, že právo na súkromie (súkromný a rodinný život) predstavuje súčasť širšieho všeobecného osobnostného práva, ktoré možno vymedziť podľa relevantných autorov ako *„súhrn právnych noriem, ktoré upravujú právo, resp. jednotlivé čiastkové práva, ktorých predmetom je osobnosť fyzickej osoby ako celku, resp. jednotlivé hodnoty tvoriace súčasť celkovej fyzickej a morálnej integrity osobnosti každej fyzickej osoby, ako individuality a suveréna, a ktorých subjekty majú voči ostatným subjektom (fyzickým či právnickým osobám) rovné právne postavenie a zásadnú autonómiu vôle“*.² Nositeľom osobnostných práv bude predovšetkým fyzická osoba, pričom všetky súčasti osobnostných práv (ochrana života a zdravia, právo na súkromie, ochrana ľudskej dôstojnosti, ochrana mena) budú spolu predstavovať komplexnosť potreby chrániť osobnosť človeka ako celku. Princíp všeobecných osobnostných práv a ich ochrany ide až tak ďaleko, že zahŕňa aj postmortálnu ochranu osobnosti zomrelého i pozostalých osôb v zmysle § 11 a nasl. OZ, a to aj na základe judikatúry Najvyššieho súdu SR.³ *„Právo na ochranu osobnosti je právo osobnej povahy, ktoré zaniká smrťou fyzickej osoby a neprechádza na dedičov. Osobám uvedeným v ustanovení § 15 OZ⁴ však vzniká originálne právo na ochranu osobnosti smrťou fyzickej osoby, do práv ktorej bolo zasiahnuté.“*⁵

1 VARGA, P. Ochrana osobnosti v kontexte historického výskumu. In: Genealogicko-heraldický hlas, roč. 26, č. 1, s. 79–85 alebo BULLA, M. Ochrana súkromia zamestnancov optikou judikatúry Súdneho dvora Európskej únie. In: Monitorovanie zamestnancov a právo na súkromný život. Bratislava: Sprint dva, 2010, s. 69–82.

2 KNAP, K. - ŠVESTKA, J. - JEHLÍČKA, O. - PAVLÍK, P. - PLECITÝ, V. Ochrana osobnosti podľa občanského práva. 4. podstatné prepracované a doplnené vyd.. Praha: Linde, 2004, s. 57, súčasne porovnaj SISKOVICHOVÁ, K. Ochrana súkromia a osobných údajov zamestnanca. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 15.

3 SISKOVICHOVÁ, K. Ochrana súkromia a osobných údajov zamestnanca. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 16.

4 § 15 OZ: „Po smrti fyzickej osoby patrí uplatňovať právo na ochranu jej osobnosti manželovi a deťom, a ak ich niet, jeho rodičom.“

5 Uznesenie Najvyššieho súdu SR z 24. októbra 2013, sp. zn. 6 Cdo 278/2013, rozsudok Najvyššieho súdu SR z 31. januára 1996, sp. zn. 3 Cdo 98/95 (R 53/1996), resp. uznesenie Najvyššieho súdu z 13. októbra 2011, sp. zn. 3 Cdo 84/2011.

Základ medzinárodnoprávnej úpravy je obsiahnutý v čl. 12 v spojitosti s čl. 3, 17 a 29 Všeobecnej deklarácie ľudských práv (hoci v právne nezáväznej podobe)⁶, ktorý predpokladá, že „nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromia, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť. Každý má právo na právnu ochranu proti takýmto zásahom alebo útokom“. V historickom právnom vývoji je následne významný okamih prijatia európskeho Dohovoru o ochrane základných ľudských práv a základných slobôd, ktorý v čl. 8 obdobne uvádza, že „každý má právo na rešpektovanie svojho súkromného a rodinného života, obdobia a korešpondencie, pričom štátny orgán nemôže do výkonu tohto práva zasahovať okrem prípadov, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinosti, ochrany zdravia alebo morálky, alebo ochrany práv a slobôd iných.“ Relevantnú medzinárodnoprávnú úpravu neskôr završuje prijatie Medzinárodného paktu o občianskych a politických právach, ktorý v čl. 16 uvádza právo každého jednotlivca na uznanie jeho právnej osobnosti a v čl. 17 analogicky deklaruje, že „nikto nesmie byť vystavený svojvoľnému zasahovaniu do súkromného života, rodiny, domova alebo korešpondencie, ani útokom na svoju česť a povesť“ a „každý má právo na zákonnú ochranu proti takým zásahom alebo útokom“.

Neskôr prijatá Charta základných práv Európskej únie právo na rešpektovanie súkromného a rodinného života v čl. 7 opätovne potvrdzuje. V čl. 8 sa Charta v porovnaní s predchádzajúcimi dokumentmi konkrétnejšie zaoberá ochranou osobných údajov, keď uvádza, že „každý má právo na ochranu osobných údajov, ktoré sa ho týkajú“, že „tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom“ a „každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu“. Dodržiavanie týchto pravidiel predpokladá zveriť ho následne do kontrolnej právomoci nezávislého orgánu.⁷

Medzi relevantné medzinárodné dokumenty, v oblasti ochrany osobných údajov v pracovnoprávnej sfére, patrí Kódex ochrany osobných údajov zamestnancov, ktorý vydala Medzinárodná organizácia práce, ktorý v čl. 1 „upravuje využívanie osobných údajov zamestnancov za účelom ochrany dôstojnosti zamestnancov a ochrany ich súkromia“. Kódex ochrany osobných údajov ďalej napr. zakazuje v čl. 5 ods. 6 hodnotenie pracovného výkonu zamestnanca výlučne na základe osobných údajov zhromaždených

6 Všeobecná deklarácia ľudských práv nemá záväzný charakter, jej prínos spočíva skôr v unifikácii zoznamu katalógu ľudských práv na medzinárodnej úrovni.

7 Ďalšiu relevantnú právnu úpravu možno nájsť napr. v čl. 16 ods. 1 Dohovoru o právach dieťaťa („žiadne dieťa nesmie byť vystavené svojvoľnému zasahovaniu do svojho súkromného života, rodiny, domova alebo korešpondencie ani nezákonným útokom na svoju česť a povesť“), v čl. 4 ods. 3 Dodatkového protokolu k Európskej sociálnej charte („pri zabezpečovaní primeranej pomoci starším osobám žijúcim v príslušných zariadeniach pre dôchodcov bolo rešpektované aj ich súkromie“) alebo v Dohovore o ľudských právach a biomedicíne (ochrana súkromného života pacientov v súvislosti s informáciami o ich zdraví) a pod.

prostredníctvom elektronického sledovania alebo v čl. 13 zakazuje, aby sa zamestnanci vzdali svojho práva na ochranu súkromia.⁸

Základným východiskom pre teoretické vymedzenie práva na súkromie zamestnanca na národnej úrovni sa stáva Ústava SR, vychádzajúca z vyššie popísanej medzinárodno-právnej úpravy, ktorá v II. hlave, čl. 16 ods. 1, čl. 19 ods. 2 a 3, čl. 21 ods. 1 až 3 a čl. 22 ods. 1 a 2 ako súčasť základných ľudských práv a slobôd uvádza právo na súkromný a rodinný život fyzickej osoby. Ústava SR bližšie právo na súkromie a jeho vlastný rozsah nedefinuje, generálne mu však zaručuje ochranu pred neoprávneným zasahovaním zo strany tretích osôb alebo štátnych orgánov. Obdobne sa rovnaká ochrana poskytuje fyzickej osobe v oblasti ochrany obydli, neoprávneného zhromažďovania, zverejňovania alebo iným zneužívaním údajov o fyzickej osobe alebo listového tajomstva, tajomstva dopravovaných správ a iných písomností a ochrany osobných údajov. Vzájomný vzťah základného ľudského práva a slobody a jeho ochrany, resp. medzi nimi navzájom, možno dohľadať v relevantnej judikatúre slovenských súdnych inšancií. Ústavný súd SR v tejto súvislosti vyslovuje právny názor, že *“všetky základné práva a slobody sa chránia len v takej miere a rozsahu, kým uplatnením jedného práva alebo slobody nedôjde k neprimeranému obmedzeniu, či dokonca popretiu iného práva alebo slobody”, resp. inej hodnoty ústavnoprávnej povahy.* Zabezpečenie rovnováhy, napr. medzi záujmami zamestnávateľa a zamestnanca, tak bude musieť byť podrobené prísnemu posudzovaniu primeranosti obmedzenia každého základného ľudského práva a ich vzájomnej interakcii. Obdobne sa v tejto súvislosti vyjadruje aj Najvyšší súd SR, ktorý vníma zásadu primeranosti a neskoršie spomínanej proporcionality aj v kontexte samotného zásahu do základného ľudského práva a slobody a jeho ospravedlnenia, keď uvádza, že *„ústavným rámcom ochrany osobnostných práv je čl. 19 Ústavy Slovenskej republiky, v zmysle ktorého každý má právo na zachovanie ľudskej dôstojnosti, osobnej cti, dobrej povesti, ochranu mena, ochranu pred neoprávneným zasahovaním do súkromného a rodinného života ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe. Uplatňovanie týchto základných práv a slobôd a ich právna ochrana musia byť proporcionálne a vzájomne vyvážené tak, aby sa nadmernou ochranou jedného práva nad únosnú mieru nepotlačila ochrana iného práva. To znamená, že ani existencia zásahu do osobných práv nemusí nevyhnutne viesť k záveru o neoprávnenosti takéhoto zásahu, ak bol dôsledkom uplatňovania iného základného práva a vzhľadom na okolnosti uplatňovania iného základného práva, nepresiahol hranice primeranosti“*¹⁰

Právo na súkromie v nadväznosti na jednotlivé uvádzané medzinárodné i národné relevantné právne predpisy nie je explicitne definované, ale je zohľadnené vo viacerých samostatných základných ľudských právach a slobodách. Existuje niekoľko právnych

8 MORÁVEK, J. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer ČR, 2013, s. 94.

9 Nález Ústavného súdu SR z 27. februára 1997, sp. zn. PL 7/96, resp. nález Ústavného súdu SR z 8. apríla 2010, sp. zn. IV. 362/09 alebo nález Ústavného súdu SR zo 16. mája 2012, sp. zn. I. 104/2012-26 a pod.

10 Rozsudok Najvyššieho súdu SR zo dňa 19. mája 2010, sp. zn. 5 Cdo 108/2009.

teórií, ako možno vnímať právo na súkromie.¹¹ Všeobecne ho možno vnímať ako základné osobnostné právo fyzickej osoby. Právo na súkromný a rodinný život predstavuje „osobné súkromie človeka (osobnú sféru jednotlivca, teda napr. údaje týkajúce sa identifikácie pohlavia, mena, sexuálnej orientácie a sexuálneho života), tak i právo každého človeka na vytváranie a rozvíjanie vzťahov s ďalšími ľudskými bytosťami (súkromnej i profesijnej povahy, akási zóna interakcie zamestnanca s inými jednotlivcami)“. Niektorí autori dokonca rozlišujú pozitívnu a negatívnu zložku práva na súkromie, pričom pozitívnu zložku tvorí právo fyzickej osoby rozhodnúť sa podľa vlastného uváženia, či a v akom rozsahu a akým spôsobom majú byť skutočnosti z jej života sprístupnené iným subjektom. Negatívna zložka pritom zahŕňa právo brániť sa proti neoprávneným zásahom do súkromnej sféry zo strany tretích osôb.¹² Na ilustráciu podobný právny názor pri vymedzení práva na súkromie zastáva aj Ústavný súd SR, ktorý uvádza, že „predmetné práva a princípy (rozumejústavný princíp slobody a realizácia základných ľudských práv a slobôd s inými fyzickými osobami) *garantujú istú „vnútornú sféru“, v ktorej môže jednotlivec žiť podľa vlastných predstáv a vylúčiť z nej „vonkajší svet“ a sféru, v ktorej sa môže jednotlivec slobodne rozvíjať, realizovať svoju osobnosť a vstupovať do vzťahov, ako aj rozvíjať vzťahy s inými osobami. Právo na súkromie a na ochranu súkromného života, v spojení s princípom slobody, tak v tom najzákladnejšom vymedzení, opierajúc sa aj o základné právo na ľudskú dôstojnosť, garantuje jednotlivcovi možnosť autonómneho sebaurčenia*“.¹³

Previazanosť a vzájomnú interakciu súkromného a rodinného života, t. j. logické odôvodnenie, prečo má zamestnanec právo dovoľávať sa ochrany súkromia aj na pracovisku, možno demonštrovať na jednom z kľúčových rozhodnutí¹⁴ Európskeho súdu pre ľudské práva, ktoré uvádza, že „súd nepokladá za možné, ani nutné pokúsiť sa o vyčerpávajúcu definíciu pojmu súkromný život. Bolo by príliš restriktívne limitovať tento pojem na „vnútorný okruh“, v ktorom jedinec žije vlastný osobný život podľa svojich predstáv, a úplne z neho vylúčiť svet, nezahrnutý do tohto okruhu. Rešpektovanie súkromného života musí do určitej miery rovnako zahŕňať i právo vytvárať a rozvíjať vzťahy s ostatnými

11 Autori uvádzajú len teoretické vymedzenia práva na súkromie, ktoré majú umožniť čitateľovi získanie základnej orientácie v spracovanej problematike s cieľom neskoršieho lepšieho pochopenia predkladaných pracovnoprávných súvislostí. Cieľom autorov nebolo podať vyčerpávajúci výklad pojmu práva na súkromie vo všeobecnom občianskoprávnom teoreticko-vednom zmysle.

12 KNAP, K. - ŠVESTKA, J. - JEHLÍČKA, O. - PAVLÍK, P. - PLECITÝ, V. Ochrana osobnosti podle občanského práva. 4. podstatně prepracované a doplněné vyd.. Praha: Linde, 2004, s. 57, súčasne porovnaj SISKOVICOVÁ, K. Ochrana súkromia a osobných údajov zamestnanca. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 22.

13 Nález Ústavného súdu SR zo 4. decembra 2007, sp. zn. PL ÚS 12/01.

14 Rozhodnutia ESĽP vo veci Niemitz Niemietz c/a Nemecko. Bližšie - ČAPEK, J. Evropský soud a Evropská komise pro lidská práva. Praha: Linde Praha a.s., 1995, s. 445 alebo Perry c/a the Velká Británie, Application no. 63737/00.

V uvedenej súvislosti možno dohľadať i ďalšiu bohatú judikatúru ESĽP a SD EÚ (kľúčovo najmä Klaas a ostatní proti Spolkovej republike Nemecko (6. 9. 1978, A28) alebo Chappel proti Spojenému kráľovstvu (30. 3. 1989, A 152), Halford proti Spojené kráľovstvo (25. 6. 1997, 20605/92), Copland proti Spojené kráľovstvo (3. 4. 2007, 62617/00), Uzun proti Nemecko (2. 9. 2010, 35623/05), Rotaru proti Rumunsko (4. 5. 2000, 28341/95) a pod.

ľudskými bytosťami. Zdá sa, že neexistuje dôvod, aby takto chápaný pojem súkromný život vylučoval činnosti profesijnej a obchodnej povahy, pretože práve v priebehu svojej pracovnej aktivity má väčšina ľudí najväčšiu príležitosť rozvíjať vzťahy s vonkajším svetom“.

Z judikatúry ESLP ďalej vyplýva, že zamestnanec sa nemôže nikdy vzdať úplne svojho práva na súkromie. Za súkromie sa preto súčasne považuje aj sféra, o ktorej sa zamestnanec oprávnené a primerane domnieva, že predstavuje jeho súkromie, napriek skutočnosti, že sa výkon jeho práce uskutočňuje v kolektívnom prostredí (spolupracovníci alebo klienti zamestnávateľa). Zamestnancovi je však neustále ponechané primárne oprávnenie rozhodnúť sa, do akej miery sprístupní svoju výsostne súkromnú sféru druhej osobe (spravidla ide o jeho zamestnávateľa).¹⁵ Z uvedeného vyplýva, že právo na súkromie v rôznych poňatiach môže zahŕňať ochranu rodinného života, súkromie obydli, listové tajomstvo, ako aj ochranu cti, povesť človeka, či ochranu pred neoprávneným zhromažďovaním údajov o osobe nielen v mimopracovnom, ale aj pracovnom prostredí, v rámci ktorého môže prichádzať rovnako k neoprávneným zásahom do práva na súkromie zamestnanca.¹⁶ Oprávnenie zamestnanca však nie je absolútne a šírka jeho oprávnenia rozhodovať o sprístupnení súkromia zamestnávateľovi sa mení v závislosti od realizovanej činnosti pracovného charakteru pre zamestnávateľa. Možnosť zamestnanca rozhodovať napr. o listovom tajomstve, alebo napr. o tajomstve správ podávaných telefónom sa do značnej miery redukuje pri činnostiach, ktoré majú byť svojou povahou činnosťami pracovnými.¹⁷

S ohľadom na ustanovenie čl. 16 ods. 1 Ústavy SR, judikatúru ESLP i judikatúru ÚS SR je nevyhnutné vymedziť aj podmienky oprávnenosti a možnosti zásahu do súkromia fyzickej osoby (zamestnanca). ÚS SR, aj na základe ustálenej judikatúry ESLP, v tejto súvislosti predpokladá, že pri každom zásahu do súkromia fyzickej osoby treba skúmať jeho legalitu, legitimitu a proporcionalitu,¹⁸ pričom však ÚS SR jednoznačne uvádza spôsob prístupu pri adopcii judikatúry ESLP do národného právneho poriadku tak, že „zásahy do práva na súkromie sa v zmysle judikatúry ESLP vykladajú v určitej logickej nadväznosti, resp. postupnosti. Predovšetkým sa skúma, či daný skutkový stav možno *ratione materiae* považovať za súčasť práva na súkromie. Po kladnej odpovedi na túto otázku treba skúmať, či zásah bol legálny. V ďalšom sa potom skúma, či bol zásah legitímny a napokon, či bol proporcionálny. Ak sa dospeje k negatívnej odpovedi na niektorú z týchto otázok, ďalej sa už v skúmaní problematiky nepokračuje.“¹⁹ Neskoršie vymedzenú triedu posudzovania prípustnosti zásahu do práva na súkromie z materiálneho hľadiska

15 ŠTEFKO, M. K problému sledování vlastních zaměstnanců. In: *Právo a zaměstnání č. 1/2005*, s. 7 až 11.

16 MURA, L. – ŽULOVÁ, J. – MADLEŇÁK, A.: Strategic management and management of personnel costs: employing young people in the Slovak Republic. In: *Problems and perspectives in management*. roč. 14, č. 1, 2016, s. 79-84.

17 Rozhodnutie Ústavného súdu ČR z 31. marca 2009, sp. zn. I. ÚS 452/09 alebo porovnaj rozsudok Nejvyššího soudu ČR zo 16. augusta 2012, sp. zn. 21 Cdo 1771/2011.

18 Nález Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 117/07.

19 Nález Ústavného súdu SR zo 14. júna 2006, sp. zn. I. ÚS 274/05, podobne však i v náleze Ústavného súdu SR z 27. mája 2008, sp. zn. III. ÚS 80/08-28.

sekundárne podporuje i znenie čl. 52 ods. 1 Charty základných práv Európskej únie, ktoré stanovuje, že „*akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo, ak je to potrebné na ochranu práv a slobôd iných*“.²⁰

Skúmanie **legality** sa odohráva v rovine posudzovania, či k realizácii zásahu prišlo v súlade s platnými právnymi predpismi, pričom sa prihliada aj na to, či právny predpis bol verejne publikovaný, a teda dostupný, a či jeho následky boli predvídateľné (zohľadnenie kvality zákonnej úpravy, ktorá predstavuje fundament zásahu do práva na súkromie – zákonná úprava zásahu do tohto práva musí byť formulovaná tak, aby nebola popretím tohto základného ľudského práva a tomu musí zodpovedať aj jej interpretácia).⁶ Legalita zásahu do súkromia znamená, že štát môže zasiahnuť do práva na súkromie len vtedy, ak takýto zásah právny poriadok pripúšťa a právna norma ho upravuje dostatočne jasne na to, aby bol za ustanovených podmienok predvídateľný.²¹ Oprávnené zásahy do práva na súkromie možno uskutočniť teda zákonom, alebo pri uplatnení zákona v súlade so všeobecnými princípmi, za ktorých možno obmedziť ústavné právo alebo slobodu jednotlivca.²² **Legitimitu** zásahu do práva na súkromie možno odvodiť z čl. 8 ods. 2 Dohovoru s výkladom, že do práva na súkromie možno zasiahnuť len vtedy, ak je to v záujme štátu z dôvodov ochrany národnej bezpečnosti, verejnej bezpečnosti, predchádzania nepokojom a zločinnosti, v záujme spoločnosti z dôvodu ochrany zdravia a morálky, zabezpečenia hospodárskeho blahobytu krajiny a v záujme jednotlivcov z dôvodu ochrany ich práv a slobôd.²³ Zásada legitimacy teda vyjadruje dôvody a podmienky, pri ktorých je možnosť obmedziť právo zamestnanca na súkromie. Stanovenie uvádzaných dôvodov však bolo príliš široké, a preto bolo neskôr precizované judikatúrou ESLP, ktorá sa zamerala predovšetkým na vymedzenie termínov „*v súlade so zákonom*“ a „*nevyhnutný v demokratickej spoločnosti*“. ESLP v tejto súvislosti uvádza, že požiadavka „*v súlade so zákonom*“ predpokladá, že právny predpis je dostatočne presný, že musí existovať prostriedok na ochranu pred ľubovoľnými zásahmi orgánov verejnej moci do záujmu, ktorému sa priznáva ochrana, ak právna úprava priznáva možnosť úvahy, rozsah a spôsob jej uplatnenia sa musí ustanoviť s dostatočnou jednoznačnosťou, aby sa zabezpečila takáto ochrana. Okrem toho, zásah do súkromia musí mať oporu vo vnútroštátnom právnom poriadku. Samotný základ v národnom právnom poriadku však nestačí: právna norma, o ktorú ide, musí byť prístupná jednotlivcovi, ktorého sa týka, pričom tento jednotlivec musí mať možnosť predvídať účinky vyplývajúce pre neho z danej právnej normy.

20 Bližšie pozri - SISKOVIČOVÁ, K. Ochrana súkromia a osobných údajov zamestnanca. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015, s. 10, ISBN 978-80-8082-932-2.

21 BARANCOVÁ, H. ed. Monitorovanie zamestnancov a právo na súkromný život. Bratislava: Sprint dva, 2010, s. 31.

22 Nález Ústavného súdu Slovenskej republiky sp. zn. PL ÚS 43/95.

23 Nález Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 117/07.

Ďalší termín „nevyhnutný“ sa podľa ESEP vzťahuje len na existenciu „naliehavej spoločenskej potreby“ vykonať daný zásah.²⁴ Zásada **proporcionality** súčasne znamená, že zasiahnuť do súkromia zamestnanca možno len keď je to nevyhnutné, keď legitímny cieľ nie je možné dosiahnuť miernejšími prostriedkami pri dodržaní zásad a princípov demokratickej spoločnosti. Keď je teda možné dosiahnuť stanovený cieľ inými prostriedkami, je nutné sa vyhnúť zásahu do súkromia zamestnancov, keďže sa ním zasahuje do jedného zo základných ľudských práv. V prípade, ak sa nedodrží čo i len jedno z vyššie uvedených kritérií zásahu do súkromia zamestnancov, možno takýto zásah považovať za nepripustný, resp. nezákonný.²⁵

1.2 Právna úprava v oblasti občianskeho a pracovného práva

Relevantnú právnu úpravu v oblasti občianskeho práva ako lex generalis vo vzťahu k ochrane súkromia fyzických osôb (a aj zamestnancov) predstavuje § 11 a § 12 Občianskeho zákonníka. Ustanovenie § 11 OZ uvádza, že „*fyzická osoba má právo na ochranu svojej osobnosti, najmä života a zdravia, občianskej cti a ľudskej dôstojnosti, ako aj súkromia, svojho mena a prejavov osobnej povahy*“. Pod prejavmi osobnej povahy pritom musíme rozumieť najmä rôzne súkromné písomnosti, fotografie či iné obrazové záznamy, ktoré zachytávajú dotknutú fyzickú osobu, alebo obsahujú informácie o nej samotnej, alebo sú prejavom jej vlastnej osobnosti (výtvarné a literárne diela, záznamy rozhovorov a pod.). V tejto súvislosti určitý návod, ako v aplikáčnej praxi vnímať rozsah zákonnej ochrany priznanej ustanovením § 11 OZ, poskytuje vo svojej judikatúre aj Najvyšší súd SR vyslovením právneho názoru, že „*výpočet uvádzaných konkrétnych zásahov do osobnostných práv fyzickej osoby nie je taxatívny, ustanovenie § 11 OZ ustanovuje len znaky, pri danosti ktorých treba určité konanie považovať za zásah do osobnosti občana. Ak sú tieto znaky dané, má každá fyzická osoba právo najmä sa domáhať, aby sa upustilo od neoprávnených zásahov do práva na ochranu jej osobnosti, aby sa odstránili následky týchto zásahov a aby jej bolo dané primerané zadostučinenie v zmysle § 13 ods. 2 OZ*“.²⁶

Ustanovenie § 12 ods. 1 OZ následne stanovuje základný generálny predpoklad použitia obsahu práva na súkromie fyzickej osoby tak, že predpokladá, že „*písomnosti osobnej povahy, podobizne, obrazové snímky a obrazové a zvukové záznamy týkajúce sa fyzickej osoby, alebo jej prejavov osobnej povahy, sa smú vyhotoviť alebo použiť len s jej privolením*“. **Zverejnenie týchto prejavov osobnosti fyzickej osoby je viazané na súhlas dotknutej fyzickej osoby.**

Výnimku zo všeobecnej premisy súhlasu fyzickej osoby so zverejnením a použitím prejavov svojej vlastnej osobnosti v zmysle vyššie naznačenej definície predstavujú tzv. zákonné licencie, t. j. OZ v § 12 ods. 2 a ods. 3 vymedzuje subjekty, ktoré môžu použiť

24 MICHALÍČEK, F. Právo na súkromie zamestnancov v judikatúre Slovenskej republiky a Českej republiky. In: Societas et Iurisprudentia, č. 1, 2014, s. 131-146.

25 MICHALÍČEK, F. Právo na súkromie zamestnancov v judikatúre Slovenskej republiky a Českej republiky. In: Societas et Iurisprudentia, č. 1, 2014, s. 131-146.

26 Rozsudok Najvyššieho súdu SR z 19. mája 2010, sp. zn. 5 Cdo 108/2009.

registrované prejavy osobnosti fyzickej osoby bez jej súhlasu na právnom poriadkom stanovené účely.²⁷

V zásade rozoznávame dva druhy týchto zákonných licencií, a to:

- zákonnú licenciu použitia týchto prejavov na úradné účely na základe zákona (napr. použitie listiny na dokazovanie na súde, alebo pri potrebe úradnej identifikácie a pod.), alebo
- zákonnú licenciu na vedecké a umelecké účely, alebo pre potreby tlačového, filmového, rozhlasového a televízneho spravodajstva (tzv. novinárska licencia).

V oboch prípadoch sa predpokladá dodržanie a sledovanie účelu použitia prejavu osobnosti (použitie bez súhlasu fyzickej osoby môže smerovať len k naplneniu zákonom stanoveného účelu) a primeranosti použitia prejavu osobnosti (pri použití prejavu osobnosti bez jej súhlasu nesmie prísť k porušeniu oprávnených záujmov tejto fyzickej osoby, napr. použitie by bolo dehonestujúce a neprimerané).²⁸ V oboch prípadoch použitia registrovaných prejavov osobnosti bez ich súhlasu musí existovať iný záujem, ktorý má prednosť, t. j. preváži nad záujmom ochrany práva na súkromie fyzickej osoby (v zmysle uvádzaného Dohovoru o ochrane základných ľudských práv a základných slobôd môže ísť o národnú bezpečnosť, ochranu verejnej bezpečnosti, ochranu verejného zdravia a pod.).

Možnosti ochrany sa v prípade občianskeho práva sústreďujú najmä na oblasť požiadavky na upustenie od neoprávnených zásahov do práva na ochranu osobnosti, odstránenia následkov takýchto neoprávnených zásahov, požiadavky na primerané zadosťučinenie, alebo pokiaľ bola v značnej miere znížená dôstojnosť fyzickej osoby alebo jej vážnosť v spoločnosti, má táto fyzická osoba tiež právo na náhradu nemajetkovej ujmy v peniazoch. V tejto súvislosti existujúca národná judikatúra vyjasňuje aj formy zásahu do osobnostných práv fyzickej osoby, pred ktorými právny poriadok poskytuje spomínanú právnu ochranu. Právna ochrana v zmysle Ústavy SR a OZ tak bude poskytnutá bezpochyby ako pred aktívnym konaním, tak aj pasívnym správaním sa (zdržanie sa konania alebo jeho opomenutie), ktoré má v OZ uvedené znaky. Týmito znakmi je predovšetkým neoprávnenosť zásahu (neoprávneným nie je zásah do osobnostnej sféry, ak sú dané okolnosti vylučujúce protiprávnosť konania, napr. výkon práva, plnenie povinnosti, svojpomoc, nutná obrana či krajná núdza) a tiež jeho objektívna spôsobilosť negatívne dopadnúť na osobnosť fyzickej osoby.²⁹

27 HRUŠOVSKÁ, V. – OLŠOVSKÁ, A. Whistleblowing na pracovisku – právna úprava, teória a prax na Slovensku. In: Whistleblowing. Praha: Wolters Kluwer CR, 2013, s. 127 – 143.

28 LAZAR, J. a kol. Občianske právo hmotné. Bratislava: Iura edition, 2006, s. 186 a násl.

29 Porovnaj všeobecný prístup k ochrane osobnosti - Rozsudok Najvyššieho súdu SR z 26. septembra 2013, sp. zn. 3 Cdo 228/2012, resp. rozsudok Najvyššieho súdu SR z 19. mája 2010, sp. zn. 5 Cdo 108/2009 alebo rozhodnutia Najvyššieho súdu SR z 15. decembra 2011, sp. zn. 3 Cdo 108/2011, 29. júna 2009, sp. zn. 3 MCdo 3/2008, 19. mája 2010, sp. zn. 5 Cdo 108/2009 a z 27. novembra 2009, sp. zn. 5 Cdo 83/2008.

Relevantnú právnu úpravu v oblasti pracovného práva ako *lex specialis* predstavujú ustanovenia čl. 11 a § 13 Zákonníka práce. ZP vychádzajúc z medzinárodných dokumentov i ÚS SR konkretizuje v čl. 11 charakter (osobných) údajov, ktoré môže zamestnávateľ o zamestnancovi zhromažďovať a v § 13 ods. 4 vymedzuje príčinnú súvislosť, pre ktorú prichádza zo strany zamestnávateľa k zhromažďovaniu týchto údajov o zamestnancovi s konkretizáciou spôsobu, miesta a formy ich zhromažďovania s existenciou participatívneho prístupu zo strany zástupcov zamestnancov. Takéto rozdelenie právnej úpravy v ZP do dvoch samostatných ustanovení je relatívne nové s účinnosťou od 1. januára 2013. Pôvodné znenie čl. 11 Základných zásad ZP sa rozdelilo a modifikovalo do dvoch samostatných ustanovení, pričom ochrana súkromia zamestnanca získala normatívny charakter v podobe § 13 ods. 4 ZP. Osobitný právny rámec ochrany súkromia v ZP treba vnímať vo vzájomnej väzbe a v rozlišovaní typu získavaných údajov, prostriedkov použitých k ich získaniu a situácie, v rámci ktorej prichádza k zhromažďovaniu týchto údajov o zamestnancovi (napr. v predzmluvných vzťahoch, počas trvania pracovného pomeru alebo po jeho skončení).

Zamestnávateľ môže rôznymi monitorovacími prostriedkami a v rôznych situáciách a príčinných dejoch získavať o zamestnancovi len osobné údaje súvisiace s jeho kvalifikáciou a profesionálnymi skúsenosťami a údaje, ktoré môžu byť významné z hľadiska práce, ktorú má zamestnanec vykonávať, vykonáva alebo vykonával.

Zákonník práce stanovuje generálny zákaz narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa. Zamestnávateľ, ktorý chce získavať údaje o zamestnancoch monitorovacími prostriedkami v zmysle § 13 ods. 4 Zákonník práce, musí mať na takúto činnosť tzv. vážny dôvod.³⁰ Pojem vážny dôvod nie je v Zákonníku práce legálne definovaný a jeho vymedzenie sa odvíja od záujmu zamestnávateľa, napr. v snahe o ochranu vlastného majetku pri výskyte krádeží, inom protiprávnom konaní, ochrana obchodného tajomstva, ochrana hodnôt v predmete činnosti zamestnávateľa. Takýto vážny dôvod musí bezprostredne spočívať v osobitnej povahe činnosti zamestnávateľa, a preto vážny dôvod má prísne individuálny charakter. Zamestnávateľ nemusí disponovať súhlasom zamestnanca so zásahom do jeho súkromia, Zákonník práce však vyžaduje jeho predchádzajúce upozornenie zamestnávateľom. Predmetom takéhoto upozornenia má byť poskytnutie informácie o charaktere kontroly (zásahov do súkromia), dobe jej trvania a použitých prostriedkoch. Odporúča sa vymedziť si takéto vážne dôvody vo vnútropodnikových organizačných aktoch, resp. v kolektívnej alebo pracovnej zmluve zamestnanca. Predchádzajúce upozornenie zamestnávateľa, vo väzbe na vážne dôvody, je nevyhnutné vykladať tak, že existencia vážnych dôvodov sa vzťahuje k okamihu začatia monitorovania zamestnancov (zásahy do súkromia, zhromažďovanie osobných údajov o zamestnancovi), a nie k povinnosti zamestnávateľa vopred upozorniť zamestnancov. Zamestnávateľ je povinný upozorniť zamestnancov

30 Pozri aj DOLOBÁČ, M. 2016. Kontrola elektronických komunikačných prostriedkov v pracovnoprávných vzťahoch. In *Právo, obchod, ekonomika VI.: zborník príspevkov z vedeckej konferencie*: 26. - 28. októbra 2016, Vysoké Tatry. - Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016, s. 145-152.

vždy, keď má záujem o zavedenie monitorovacieho systému, a nielen vtedy, keď by mal na jeho zavedenie vážny dôvod. V takomto prípade neexistencie vážnych dôvodov by vôbec nemohol získavať údaje o svojich zamestnancoch, pretože by nesplnil zákonnú podmienku jeho zavedenia.

Popri povinnosti zamestnávateľa vopred informovať zamestnanca o zásahoch do jeho súkromia prostredníctvom monitorovacieho systému, je zamestnávateľ povinný prerokovať so zástupcom zamestnancov pôsobiacim u zamestnávateľa zavádzaný kontrolný mechanizmus. Proces prerokovania sa spravuje ustanovením § 237 Zákonníka práce, pričom Zákonník práce vymedzuje v § 13 ods. 4 jeho obsahovú náplň na oboznámenie zástupcov zamestnancov zo strany zamestnávateľa o rozsahu uskutočňovanej kontroly, spôsoboch jej uskutočnenia a dobe jej trvania. Nesúhlas zástupcov zamestnancov so zavedením kontrolného mechanizmu zamestnávateľa nezaväzuje, musí však zachovať účelnosť, transparentnosť a primeranosť jeho zavedenia vo vzťahu k dôvodom, pre ktoré kontrolný systém zavádza. Kontrola by mala byť vykonávaná iba v nevyhnutnom rozsahu, aby neprišlo k zásahu do práva na ochranu osobnosti zamestnanca, mala by byť realizovaná v rámci pracovného času a priamo na pracovisku zamestnávateľa, kontrolu by mal vykonávať osobne zamestnávateľ alebo ním poverený vedúci zamestnanec (prípadne SBS). Odporúča sa obsiahnuť všetky potrebné informácie o kontrolnom mechanizme, predovšetkým s ohľadom na charakter a spôsob výkonu kontroly, vo vnútorných predpisoch zamestnávateľa (pracovný poriadok), v kolektívnej zmluve alebo v pracovnej zmluve zamestnanca.³¹

1.3 Právna úprava v oblasti ochrany osobných údajov – všeobecné nariadenie o ochrane údajov

Právna úprava ochrany práva na ochranu osobných údajov pred ich neoprávneným spracúvaním, alebo iným zneužívaním, je v oblasti samotnej ochrany osobných údajov a pravidiel upravujúcich spracúvanie osobných údajov premietnutá do zákona o ochrane osobných údajov, do ktorého bola prevzatá právna regulácia obsiahnutá v smernici 95/46/ES. V súčasnosti sa uplatňuje tzv. prechodné obdobie, keď 4. mája 2016 bolo v Úradnom vestníku Európskej únie zverejnené 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). **Nové nariadenie je uplatniteľné od 25. mája 2018³², do uvedeného okamihu sa naďalej aplikuje zákon o ochrane osobných údajov.**

Prijatie všeobecného nariadenia o ochrane údajov, s odkazom na jeho odôvodnenie (recitály), malo za cieľ zabezpečiť konzistentnú a vysokú úroveň ochrany fyzických

31 Podrobnejší výklad k uvedeným ustanoveniam bude premietnutý do právneho výkladu v rámci ostatných kapitol publikácie v zmysle jej logického členenia.

32 Nariadenie je osobitný typ právneho aktu Európskej únie, ktoré má priamy účinok vo všetkých členských štátoch Európskej únie, t. j. priamo zaväzuje dotknuté osoby na území členských štátov bez potreby jeho osobitného premietnutia do národnej legislatívy.

osôb pred neoprávneným zásahom do ich práv a slobôd. Základné princípy a ciele formulované v smernici 95/46/ES zostávajú naďalej zachované, avšak prostredníctvom jej transpozície do práva členských štátov nebolo možné zamedziť rozdielom pri vykonávaní ochrany osobných údajov v Únii. Všeobecné nariadenie o ochrane údajov má zabezpečiť spresnenie práv dotknutých osôb a povinností prevádzkovateľov alebo sprostredkovateľov, ktorí osobné údaje spracúvajú a účinnú ochranu osobných údajov v rámci celej Únie. Všeobecné nariadenie o ochrane osobných údajov zjednocuje rozsiahlu nekonzistenciu právnych úprav v rámci jednotlivých členských štátov Únie, ktoré aj napriek napr. spoločným historickým koreňom (Česko a Slovensko) neboli zjednotené čo do obsahovej, tak aj do výkladovej stránky. Tieto rozdiely boli spôsobené rozdielnou implementáciou predchádzajúcej právnej úpravy smernice 95/46/ES, ktorá sa v roku 1995 stala nosným nástrojom štandardizácie úpravy práv a povinností pri spracúvaní osobných údajov v Únii.

1.3.1 Nový legislatívny rámec pri ochrane osobných údajov

Implementácia všeobecného nariadenia o ochrane osobných údajov do slovenského právneho poriadku sa realizuje prostredníctvom nového zákona o ochrane osobných údajov, ktorý bude tvoriť nový legislatívny rámec pre ochranu osobných údajov v Slovenskej republike³³. Novým zákonom sa zároveň transponuje smernica³⁴ do právneho poriadku Slovenskej republiky.

Nový zákon o ochrane osobných údajov predstavuje komplexný právny rámec ochrany osobných údajov pre spracovateľské operácie s osobnými údajmi, ktoré sa vykonávajú v rámci činností, ktoré nespádajú do pôsobnosti práva Európskej únie, a ktorý je zosúladený a do najvyššej možnej miery konzistentný s právnou úpravou ochrany osobných údajov v nariadení. Týmto postupom sa predchádza vytvoreniu právneho vákua v oblasti ochrany osobných údajov, keďže návrhom zákona bude zrušený zákon o ochrane osobných údajov a dva vykonávacie predpisy Úradu k nemu prislúchajúce.

Nová právna úprava v prvej a druhej časti návrhu zákona stanovuje pravidlá spracúvania osobných údajov pre prevádzkovateľov a sprostredkovateľov, na ktoré sa **nevzťahujú** pravidlá ochrany fyzických osôb pri spracúvaní osobných údajov a pravidlá týkajúce sa voľného pohybu osobných údajov podľa všeobecného nariadenia o ochrane

33 V čase prípravy publikácie prebiehal legislatívny proces schvaľovania návrhu nového zákona o ochrane osobných údajov, zaradenom pod číslom parlamentnej tlačky 704; návrh nového zákona bol v druhom čítaní. Vzhľadom na to, že zákonom sa okrem iného implementuje nariadenie, v tejto fáze legislatívneho procesu sa neočakávajú významné zmeny pre prevádzkovateľov, na ktorých sa pri spracúvaní osobných údajov nariadenie vzťahuje.

34 Smernica Európskeho parlamentu a rady (EÚ) č. 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4. 5. 2016), ktorá spolu s ďalšími ustanoveniami nového zákona o ochrane osobných údajov vytvorí harmonizovaný a konzistentný právny rámec pre spracúvanie osobných údajov pre tie subjekty, na ktoré sa nariadenie nevzťahuje [čl. 2 ods. 1 písm. d) nariadenia].

údajov. Tretia časť novej právnej úpravy stanovuje pravidlá spracúvania osobných údajov pre prevádzkovateľov, ktorými sú **príslušné orgány** pri spracúvaní osobných údajov na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií na základe transpozície smernice.

Štvrtá časť navrhovanej právnej úpravy vo svojich ustanoveniach je tzv. **implementačnou/vykonávacou** časťou zákona, ktorá dopĺňa osobitné pravidlá spracúvania osobných údajov stanovené nariadením. Návrh zákona vo vzťahu k spracúvaniu, v rámci tejto časti, upravuje spracovateľské operácie, ktoré nariadenie výslovne ukladá, alebo umožňuje jednotlivým členským štátom upraviť osobitnou vnútroštátnou úpravu, na základe tzv. splnomocňujúceho ustanovenia nariadenia.

Konkrétne ide o osobitné úpravy spracúvania osobných údajov, ktoré upravujú:

- pravidlá spracúvania osobných údajov na akademické, umelecké, literárne účely, vrátane zavedenia primeraných záruk,
- pravidlá pre spracúvanie osobných údajov pre potreby informovania verejnosti masovokomunikačnými prostriedkami,
- pravidlá spracúvania osobných údajov v súvislosti so zamestnaním,
- spracúvanie národného identifikačného čísla (rodné číslo),
- podmienky získavania osobných údajov o fyzickej osobe od inej fyzickej osoby do informačného systému,
- podmienky spracúvania osobných údajov o osobe, ktorá už nežije (odlišná úprava oproti nariadeniu, ktoré údaje o nežijúcej osobe nepovažuje za osobné údaje),
- postup pri prijímaní primeraných bezpečnostných opatrení a posúdení vplyvu (odkazuje na medzinárodné normy a štandardy).

Zároveň nariadenie určuje členským štátom prijať pravidlá týkajúce sa postavenia a organizácie dozorného orgánu v rámci vnútroštátneho právneho poriadku členského štátu, ako aj procesné pravidlá pre výkon kontroly a konania o ochrane osobných údajov dozorným orgánom.

Piata časť návrhu zákona upravuje postavenie Úradu, jeho pôsobnosť, právomoci a jeho personálny substrát. Ďalej upravuje kódexy správania, certifikáty, proces akreditácie, monitorujúceho subjektu a certifikačného subjektu. Tretia hlava piatej časti je venovaná kontrole, štvrtá hlava konaniu o ochrane osobných údajov. Piata hlava je venovaná pokutám, správnym deliktom a poriadkovým pokutám, teda sankciám. Šiesta časť upravuje spoločné, prechodné a záverečné ustanovenia.

Obsah návrhu nového zákona o ochrane osobných údajov v niektorých oblastiach plne recipuje právnu úpravu vyplývajúcu z nariadenia bez zmeny, t. j. neodchyľuje sa, hoci nariadenie takúto možnosť v niektorých prípadoch pripúšťa. Hoci na tento prístup zákonodarcu môžeme mať rôzne názory, musíme si uvedomiť, že nariadenie vo svojom článku 2 ods. 2 písm. a) vymedzuje svoju pôsobnosť negatívne, a to tak, že sa nevzťahuje na spracúvanie osobných údajov v rámci činnosti, ktoré nepatria do pôsobnosti úniové-

ho práva. Znamená to, že nariadenie by sa v plnom rozsahu podľa súčasného stavu delby kompetencií medzi EÚ a členskými štátmi malo vzťahovať na tri druhy kompetencií: i) výlučné právomoci,³⁵ⁱⁱ⁾ spoločné kompetencie³⁶ a iii) podporné, koordinačné a doplnkové činnosti.³⁷ Na zostatkové právomoci, t. j. právomoci členských štátov, ktoré neboli zakladajúcimi zmluvami prenesené na Úniu, sa nariadenie nevzťahuje. Doslovným prevzatím článkov a ustanovení z nariadenia do vnútroštátneho právneho predpisu tak *de facto* bola pôsobnosť nariadenia rozšírená aj na činnosti, ktoré nepatria do pôsobnosti Únie, samozrejme, nie v rozsahu všetkých zostatkových právomocí členského štátu, ale len v takom rozsahu, ako svoju vecnú a územnú pôsobnosť vymedzuje nový zákon o ochrane osobných údajov. Ani nariadenie, ani nový zákon o ochrane osobných údajov tak napríklad nemožno aplikovať na spracúvanie osobných údajov pri činnostiach, ako je zabezpečenie národnej bezpečnosti. Podľa § 3 ods. 5 písm. b) a c) sa nový zákon o ochrane osobných údajov *nevzťahuje na spracúvanie osobných údajov Slovenskou informačnou službou, Vojenským spravodajstvom, ani Národným bezpečnostným úradom na účely vykonávania bezpečnostných previerok a na účely zabezpečovania podkladov pre rozhodovanie Súdnej rady SR o splnení predpokladov sudcovskej spôsobilosti*. Rovnako tak sa naďalej pravidlá ochrany osobných údajov nevzťahujú na spracúvanie osobných údajov výlučne na osobné alebo domáce činnosti (osobný adresár, korešpondencia, monitorovanie výlučne obydliá, záhrady).³⁸ V poslednom uvedenom prípade sa neaplikujú ustanovenia zákona o ochrane osobných údajov, avšak platí, že ani s takto získanými alebo držanými osobnými údajmi (adresár) nie je nikto oprávnený nakladať svojvoľne. Každý, kto spracúva osobné údaje výlučne pre osobnú potrebu, musí pri nakladaní s nimi dbať, aby neoprávnene nezasiahol do práva na ochranu súkromia iných. V prípade, kedy sa na spracúvanie osobných údajov nevzťahuje zákon o ochrane osobných údajov, vzťahujú sa na ne ustanovenia iných právnych predpisov, napr. Občianskeho zákonníka.

V závere musíme pre doplnenie konštatovať, že zákon o ochrane osobných údajov je všeobecným právnym predpisom (*lex generalis*) voči ostatným vnútroštátnym zákonom, ktoré upravujú ochranu osobných údajov a ktoré sú špeciálnou právnou úpravou (*lex specialis*), napríklad ZP, ktorý obsahuje ustanovenia chrániace súkromie a osobné údaje zamestnanca, a súčasne predstavuje jeden z právnych základov spracúvania osobných údajov.

35 Patrí sem colná únia, ustanovenie pravidiel hospodárskej súťaže potrebných na fungovanie vnútorného trhu, menová politika pre členské štáty, ktorých menou je euro, ochrana morských biologických zdrojov v rámci spoločnej politiky rybného hospodárstva a spoločná obchodná politika.

36 Spoločné právomoci Únie a členských štátov sa uplatňujú napr. v týchto oblastiach: vnútorný trh; sociálna politika; hospodárska, sociálna a územná súdržnosť; životné prostredie; ochrana spotrebiteľa; doprava, transeurópske siete a pod.

37 Napríklad podporné, koordinačné a doplnkové aktivity v rámci ochrany a zlepšovania zdravia ľudí, priemyslu, cestovného ruchu, kultúry, vzdelávania a pod.

38 Pozor však na zrušený právny základ, na základe ktorého bolo možné bez súhlasu spracúvať osobné údaje získané náhodne, bez splnenia požiadaviek kladených zákonom o ochrane osobných údajov, ktorými sú najmä určenie účelu a prostriedkov spracúvania, bez zámeru ich ďalšieho spracúvania v usporiadanom systéme (dokumenty obsahujúce osobné údaje nájdené na skládke odpadov).

II. Pôsobnosť GDPR a nového zákona o ochrane osobných údajov

Pôsobnosť GDPR bude založená v konkrétnom prípade vtedy, ak budú splnené predpoklady územnej, vecnej a osobnej pôsobnosti tejto právnej normy. Z hľadiska territoriality GDPR potenciálne ovplyvňuje všetky fyzické osoby v EÚ, všetky organizácie v EÚ, ktoré spracúvajú osobné údaje, ako aj organizácie mimo EÚ, ktoré spracúvajú osobné údaje týkajúce sa fyzických osôb v EÚ.

Z hľadiska vecného rozsahu sa GDPR vzťahuje na spracúvanie osobných údajov, vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie osobných údajov inými než automatizovanými prostriedkami, ak ide o osobné údaje, ktoré tvoria súčasť informačného systému, alebo sú určené na to, aby tvorili súčasť informačného systému. Informačným systémom je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe.

Z osobného hľadiska zasahuje spracúvanie osobných údajov podľa GDPR vzťahy hmotnoprávne definovaných subjektov: dotknutej osoby, prevádzkovateľa, spoločných prevádzkovateľov, sprostredkovateľa, subdodávateľa, zástupcu prevádzkovateľa/sprostredkovateľa, tretiu stranu a príjemcu.

2.1. Územná pôsobnosť

GDPR podlieha každý prevádzkovateľ (zamestnávateľ) a každý sprostredkovateľ spracúvajúci osobné údaje v rámci činnosti svojej prevádzky **usadený** na území EÚ alebo so sídlom v členskom štáte Európskeho hospodárskeho priestoru. Je irelevantné umiestnenie prostriedkov spracúvania osobných údajov, t. j. či sa spracúvanie osobných údajov fakticky vykonáva na území EÚ/EHP, alebo nie. Pôsobnosť nového zákona o ochrane osobných údajov je potom založená vo vzťahu ku každému prevádzkovateľovi so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území SR, tiež bez ohľadu na to, či sa spracúvanie osobných údajov vykonáva na území SR, alebo mimo územia SR. Rovnako je územná pôsobnosť nového zákona o ochrane osobných údajov rozšírená na miesta, kde sa na základe medzinárodného práva verejného uplatňuje právny poriadok SR. Pôjde o prípady diplomatických misií, zahraničné zastupiteľstvá štátov, či konzulárne úrady.

Usadenie sa na území EÚ znamená, že prevádzkovateľ alebo sprostredkovateľ má sídlo, miesto podnikania, organizačnú zložku, *prevádzkareň* alebo trvalý pobyt na území niektorého členského štátu EÚ. Kým sídlo podnikania, miesto podnikania, organizačná zložka, trvalý pobyt zodpovedajú rovnakým významom, ako sa bežne používajú, pojem prevádzkareň sa v zmysle judikatúry SD EÚ v prípade *C-230/14 Weltimmo*³⁹ neobmedzuje na prevádzkareň v zmysle práva obchodných spoločností. Rozhodujúca

39 C-230/14 Weltimmo s.r.o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság z 1. októbra 2015.

nie je ani právna forma prevádzkarne, či už je to pobočka, alebo dcérska spoločnosť s právnou subjektivitou a výklad tohto pojmu sa neobmedzuje ani na formálne poňatie, podľa ktorého je podnik usadený výlučne na mieste, kde je zapísaný. Prevádzkareň je miesto akejkoľvek právnej formy, z ktorého je stabilne, účinne a skutočne vykonávaná určitá činnosť. Ako faktory, ktoré môžu napomôcť určiť takú prevádzkareň, z ktorej sa účinne a skutočne vykonáva určitá činnosť, môžu slúžiť aj keď nepriamo napr. miesto, z ktorého boli osobné údaje uložené; štátna príslušnosť dotknutých osôb; miesto bydliska vlastníkov podniku, ktorý je prevádzkovateľom osobných údajov; alebo okolnosť, že služba poskytovaná týmto prevádzkovateľom údajov je zameraná na územie iného členského štátu a pod. Za prevádzkareň sa môže považovať aj jediný zástupca, pokiaľ sa vyznačuje dostatočnou úrovňou stálosti, čo je dané existenciou ľudských a technických prostriedkov nevyhnutných na to, aby sa mohli poskytovať konkrétne služby. Ak sa takáto prevádzkareň teda nachádza na území EÚ/EHS, spracúvanie osobných údajov v rámci činnosti prevádzkarne bude podliehať pravidlám GDPR.

Novým prvkom GDPR, ktorý chráni vnútorný trh EÚ, je explicitné rozšírenie jeho exteritoriálnej pôsobnosti aj na prevádzkovateľov a sprostredkovateľov usídlených mimo EÚ, ak spracúvajú osobné údaje dotknutej osoby nachádzajúcej sa na území EÚ a spracúvanie osobných údajov súvisí:

- a) s ponukou tovaru alebo služieb tejto dotknutej osobe na území EÚ bez ohľadu na to, či sa od dotknutej osoby vyžaduje platba alebo nie, alebo
- b) so sledovaním správania dotknutej osoby na území EÚ (pokiaľ sa toto správanie uskutočňuje v EÚ).

K bod a)

Z činnosti spoločnosti musí byť zrejmé, že spoločnosť svoje aktivity bude smerovať na dotknuté osoby žijúce na území EÚ. Len prístupenie webových stránok, emailovej adresy či kontaktných adries z územia EÚ, alebo použitie jazyka, ktorý sa všeobecne používa v tretej krajine, kde je prevádzkovateľ usadený, nie sú dostačujúce. Relevantnou skutočnosťou pre založenie exteritoriálnej pôsobnosti GDPR je už možnosť uskutočniť objednávku v úradnom jazyku dotknutej členskej krajiny EÚ a možnosť platby v príslušnej mene. Zistiť by sa malo, či prevádzkovateľ alebo sprostredkovateľ plánuje ponúkať služby dotknutým osobám v jednom alebo vo viacerých členských štátoch v EÚ.

K bodu b)

Pod sledovaním správania dotknutej osoby sa rozumie predovšetkým mapovanie jej správania na internete, vrátane prípadného následného využitia technologických riešení spracúvania osobných údajov, ktoré spočívajú v profilovaní fyzickej osoby na účely prijatia rozhodnutia týkajúceho sa tejto osoby, alebo na účely analýzy či predvídania osobných preferencií, správania a postojov tejto osoby (recitál č. 24 GDPR). Ide tak

o online tracking a behaviorálnu reklamu generovanú prostredníctvom internetových vyhľadávačov, či sociálnych sietí.

Prevádzkovateľ/sprostredkovateľ, ktorý nie je usadený na území EÚ, ale na ktorého sa bude vzťahovať pôsobnosť GDPR v zmysle vyššie zadefinovaných kritérií, je povinný na plnenie pravidiel ochrany osobných údajov písomne poveriť svojho **zástupcu**. Zástupcom môže byť fyzická osoba alebo právnická osoba, ktorá bude mať sídlo, miesto podnikania, organizačnú zložku, prevádzkareň alebo trvalý pobyt v niektorom členskom štáte EÚ. Zástupcu nemusí poverovať orgán verejnej moci, alebo verejnoprávna inštitúcia, a ani ten prevádzkovateľ/sprostredkovateľ, ktorý kumulatívne naplní nasledujúce podmienky:

- a.) spracúvanie osobných údajov je občasný,
- b.) nezahŕňa vo veľkom rozsahu spracúvanie osobitných kategórií osobných údajov alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku, a
- c.) nie je pravdepodobné, že s ohľadom na povahu, kontext, rozsah alebo účel spracúvania povedie k riziku pre práva fyzických osôb.

2.2. Vecná pôsobnosť

Podstatou vecnej pôsobnosti GDPR a rovnako aj zákona o ochrane osobných je, že sa vzťahuje na akékoľvek spracúvanie **osobných údajov** prevádzkovateľom. Je nepodstatné, či prevádzkovateľ spracúva osobné údaje pre nejaký účel, lebo to tak sám chce (napr. realizácia cieľovej reklamy), alebo či spracúva osobné údaje v dôsledku plnenia zákonnej povinnosti (napr. prihlásenie zamestnanca do Sociálnej poisťovne, vedenie mzdových listov). Rovnako je nepodstatný spôsob spracúvania osobných údajov. Pravidlá ochrany osobných údajov sa vzťahujú na spracúvanie osobných údajov za výlučného využitia technológií (rôzne aplikácie), za použitia kombinácie technológie a ľudského faktora (časť údajov z osobného spisu zamestnanca je vedená v počítači, časť papierovo v zložkách) i na výsostne manuálne spracúvanie (vkládanie a ukladanie osobných údajov do informačných systémov).

2.2.1. Všeobecné osobné údaje

Definícia pojmu osobné údaje sa rovná definovaniu toho, čo patrí a čo nepatrí pod pôsobnosť pravidiel o ochrane osobných údajov a je pomerne široká. Podľa § 2 nového zákona o ochrane osobných údajov sú osobnými údajmi *údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.*

V porovnaní so starým zákonom o ochrane osobných údajov sú zmeny v definícii osobného údajá nepodstatné. GDPR spresňuje koncept osobných údajov a za osobné údaje sú už považované aj rôzne online identifikátory osôb (napríklad IP adresa, cookies) a iné elektronické identifikátory (napríklad RFID technológie, či tzv. prevádzkovo-lokalizačné údaje).

Aj naďalej ide o príkladný výpočet údajov, ktoré možno považovať za osobné. Stále platí, že na to, aby sme dáta alebo skupinu dát mohli právne kvalifikovať ako osobné údaje, musia sa týkať už identifikovanej (určenej) osoby, alebo osoby priamo alebo nepriamo identifikovateľnej (určiteľnej). Osoba je identifikovateľná vtedy, keď je bez vynaloženia neprimeraného úsilia možné získať doplňujúce informácie umožňujúce jej identifikáciu. V súlade s definíciou dotknutej osoby, okrem toho, že údaj identifikuje jednotlivca, musí „sa vzťahovať“ k jednotlivcovi, t. j. údaj môže (musí) mať vplyv na konkrétnu fyzickú osobu (napr. môže jej spôsobiť ujmu). Posúdenie, či je získaný údaj osobným, je potrebné vykonať vždy v rámci konkrétného kontextu spracúvania. Napríklad informácia o tom, že zamestnanec sa zúčastnil stretnutia spoločnosti, v ktorej pracuje, nebude spĺňať kritérium osobného údajá, avšak informácia o tom, že daný zamestnanec nedostatočne reprezentoval spoločnosť (napríklad v rozpore s pokynmi) osobným údajom môže byť. Rovnako tak, ak zamestnávateľ prideliť svojim zamestnancom identifikačné číslo a cez toto číslo ich identifikuje, napríklad v súvislosti so zverejňovaním hodnotenia ich pracovného výkonu, na prvý pohľad je ťažko identifikovať konkrétného zamestnanca. Ak však zamestnávateľ číslo generuje v časovej následnosti podľa poradia, kedy do spoločnosti jednotliví zamestnanci nastúpili, pre určitý okruh ľudí so znalosťou miestnych pomerov je možné z informácie identifikovať približnú dobu pracovnoprávneho vzťahu k zamestnávateľovi a spolu s internými informáciami o pracovných pomeroch spojiť tieto informácie s konkrétnou osobou. Aby sme mohli hovoriť o tom, že na základe určitého množstva informácií je konkrétna fyzická osoba identifikovateľná, musíme vziať do úvahy všetky prostriedky (najmä finančné a personálne), u ktorých je primeraná pravdepodobnosť, že ich prevádzkovateľ, alebo iná osoba, využije na identifikáciu osoby.

Z hľadiska obsahu sú osobné údaje akýmkoľvek druhom informácií o osobe týkajúce sa jej súkromného, rodinného, pracovného i verejného života. Podoba (formát) osobných údajov, v akej sa osobné údaje pre uplatnenie pravidiel ich ochrany nachádzajú, nie je rozhodujúca (papierová, elektronická grafická, číselná, fotografická...). Zvukové a obrazové údaje je rovnako možné pokladať za osobné údaje, ak predstavujú informácie o jednotlivcovi. Osobné údaje môžu byť obsiahnuté aj v správe elektronickej pošty. Informácie nemusia byť ani pravdivé, ani preukázané, aby ich bolo možné označiť za osobné údaje.⁴⁰

40 Ku komplexnejšiemu rozboru pojmu osobný údaj pozri bližšie: Stanovisko č. 4/2007 k pojmu osobné údaje (WP 136), Metodické usmernenie Úradu pre ochranu osobných údajov SR č. 1/2013 k pojmu osobné údaje alebo tiež ŠVEC, M., VALENTOVÁ, T. Ochrana osobných údajov v pracovnoprávnych vzťahoch. Bratislava: Wolters Kluwer, 2016.

Osobným údajom nie je anonymný ani anonymizovaný údaj, preto sa na nich ani nevzťahuje zákon o ochrane osobných údajov. Anonymný údaj je údaj, ktorý sa neviaže na identifikovanú alebo identifikovateľnú fyzickú osobu. Anonymizovaný údaj je údaj, u ktorého boli odstránené všetky identifikačné prvky a ani po vynaložení primeraného úsilia už nie je možná opätovná identifikácia dotknutej osoby. Na rozdiel od anonymných a anonymizovaných údajov sú osobnými údajmi pseudonymizované údaje. Pseudonymizovaný údaj je údaj, ktorého identifikačné prvky sú nahradené jedným pseudonymom. Osobné údaje je možné priradiť konkrétnej dotknutej osobe až za použitia dodatočných informácií (šifrovacieho kľúča), ktorým ale disponuje len oprávnená osoba. Pseudonymizácia je tak proces maskovania identít.

2.2.2. Osobitná kategória osobných údajov (tzv. citlivé údaje)

Ide o údaje, ktorých spracúvanie môže pre dotknutú osobu predstavovať vyššie riziko ohrozenia práv a právom chránených záujmov. Podľa čl. 9 ods. 1 GDPR a ust. § 16 ods. 1 nového zákona o ochrane osobných údajov sa zakazuje s výnimkami uvedenými v § 16 ods. 2 spracúvanie osobitných kategórií osobných údajov. *Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia, alebo údaje týkajúce sa sexuálneho života, alebo sexuálnej orientácie fyzickej osoby.* V porovnaní so starým zákonom o ochrane osobných údajov bola definícia citlivého osobného údaje v novom zákone o ochrane osobných údajov spresnená a rozšírená. Došlo aj k spresneniu zákonnej definície biometrických údajov⁴¹ a pribudla definícia genetických údajov⁴² a údajov týkajúcich sa zdravia.⁴³

Z definície citlivých údajov sa vypustilo členstvo v politických stranách alebo politických hnutiach, ktoré však podľa nášho názoru možno zahrnúť do širšieho poňatia pojmu politické názory.

Z dôvodu svojej povahy vyžadujú citlivé údaje rozšírenú ochranu. GDPR a v nadväznosti naň zákon o ochrane osobných údajov ustanovuje vyčerpávajúcim spôsobom, kedy ich možno spracúvať a ich spracúvanie si vyžaduje prijatie špecifických záruk.

41 Biometrickými údajmi sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu, alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje, ako napr. odtlačok prsta, odtlačok dlane, biometrický snímok sietnice oka, tvar tváre a vzdialenosti jednotlivých orgánov na nej, hlas, geometria ruky, geometria štruktúry žíl ruky alebo dlane a pod.

42 Genetickými údajmi sú osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby

43 Údajmi týkajúcimi sa zdravia sú osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave.

2.2.3. Všeobecné osobné údaje a citlivé osobné údaje zamestnanca

Zamestnávateľ prichádza v praxi do kontaktu najčastejšie s týmito všeobecnými osobnými údajmi zamestnanca:

- Identifikačné údaje: meno, priezvisko, rodné priezvisko, prezývka, dátum narodenia, miesto narodenia, číslo občianskeho preukazu, číslo pasu alebo iného dokladu totožnosti, titul, štátna príslušnosť, národnosť;
- kontaktné údaje: adresa trvalého/prechodného pobytu alebo bydliska, telefónne číslo, e-mailová adresa, adresa na facebooku alebo inej sociálnej sieti;
- prevádzkové údaje: register pracovného času (t. j. údaje o čase, kedy jednotliví zamestnanci začínajú a končia pracovnú zmenu, aj údaje o prestávkach alebo čase, ktorý nie je do pracovného času zahrnutý), pracovná funkcia, identifikačné číslo zamestnanca, prístupový kód/heslo zamestnanca, online identifikátor, pracovná IP adresa;
- lokalizačné údaje: údaje určujúce geografickú polohu zamestnanca (najmä pri využívaní GPS), údaje v knihe jász služobného motorového vozidla a pod.
- identifikátory vytvárajúce ekonomickú identitu zamestnanca (údaj o mzde, číslo bankového účtu, bankové spojenie), sociálnu identitu (údaje o rodinnom stave, počte detí, dosiahnutom vzdelaní), mentálnu identitu (informácie o správaní a osobných vlastnostiach zamestnanca zachytené v pracovnom posudku).

Osobné údaje tak zahŕňajú aj subjektívne informácie, názory alebo hodnotenia, pričom tento subjektívny druh informácií tvorí značnú časť osobných údajov spracúvaných práve v sektoroch, medzi ktoré patrí oblasť zamestnania.

K citlivým osobným údajom zamestnanca možno zaradiť jeho fotografickú podobu, ak sa spracúvajú biometrické údaje, ktoré táto fotografia zachytáva; ďalej vlastnoručný podpis, rovnako vtedy, ak sa z neho získavajú behaviorálne charakteristiky; údaje o zdravotnom stave;⁴⁴ výsledky dychovej/krvnej skúšky na alkohol; potvrdenie o tehotenstve zamestnankyne; potvrdenie o invalidite; údaje o psychickej pracovnej spôsobilosti; odtlačky prstov; sken sietnice; spracúvanie hlasu zamestnanca pri monitorovaní telefónov, členstvo v odborovej organizácii.

Osobitné postavenie má spracúvanie údajov o porušení predpisov trestného práva, priestupkového práva alebo občianskeho práva (výpis/odpis z registra trestov), pretože takéto spracúvanie je možné len na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, ktoré poskytujú primerané záruky ochrany práv dotknutej osoby.

⁴⁴ Napríklad údaj o tom, že si určitý zamestnanec poranil nohu a je čiastočne práceneschopný, je citlivým osobným údajom týkajúcim sa zdravia zamestnanca. Bližšie rozhodnutie SD EÚ vo veci C-101/01 Bodil Lindqvist zo 6. novembra 2003, bod 51.

2.3. Kľúčové zásady spracúvania osobných údajov

Nakladanie s osobnými údajmi vymedzuje zákon o ochrane osobných údajov legálnym pojmom spracúvanie. Ide o široký pojem s dynamickým významom a rozsahom znamenajúci napr. *získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmenu, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa také spracúvanie vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami*. Spracúvanie osobných údajov nemožno vykladať reštriktívne a ide o demonštratívny výpočet toho, čo sa rozumie spracúvaním. Prvá spracovateľská operácia je v podstate získavanie a posledná likvidácia osobných údajov. V zásade akákoľvek manipulácia s osobnými údajmi medzitým je spracúvaním, vrátane sprístupňovania, či zverejňovania osobných údajov. Pri spracovateľských operáciách je potrebné dbať na skutočnosť, aby s osobnými údajmi bolo nakladané s náležitou opatrnosťou a zákonným spôsobom, aby manipuláciou s nimi nedošlo k neoprávnenému zásahu do práv a právom chránených záujmov dotknutých osôb (tzv. zásada zákonnosti).

V pracovnoprávných vzťahoch sa možno stretnúť so širokou škálou spracovateľských operácií. V rámci predzmluvných vzťahoch, t. j. v procesoch výberu vhodného zamestnanca a pri kreovaní zmluvných typov zakladajúcich pracovnoprávne vzťahy, zamestnávateľ *získava* osobné údaje dotknutej osoby. Následne získané osobné údaje *využíva* na realizáciu práv a hlavne plnenie povinností vyplývajúcich mu zo Zákonníka práce a ďalších právnych predpisov a *uchováva* ich po stanovené alebo určené lehoty archivácie. Po uplynutí lehôt archivácie je zamestnávateľ povinný osobné údaje *likvidovať*, a to takým spôsobom, aby osobné údaje nebolo možné viac reprodukovať ani ich obnoviť. K *poskytovaniu, sprístupňovaniu a zverejňovaniu informácií* o zamestnancoch pozri kapitolu 4.8.

2.3.1 Zásada obmedzenia účelu a zásada minimalizácie údajov

Prvý krok manipulácie s osobnými údajmi spočíva vo vymedzení dôvodu, prečo chceme/potrebuje spracúvať osobné údaje. Ide o určenie účelu spracúvania osobných údajov. Účel určuje sám prevádzkovateľ (v pracovnoprávných vzťahoch pravidelne zamestnávateľ), alebo mu účel vyplýva priamo z právneho predpisu. Nemožno určiť hocijaký účel. Osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom. Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať. Pre zamestnanca musí byť jednoznačne zrejmé, na čo poskytuje zamestnávateľovi svoje osobné údaje.

Určenému účelu, alebo účelu stanovenému osobitným predpisom potom zodpovedá zoznam a rozsah osobných údajov, ktoré možno spracúvať, čo je vyjadrením zásady

minimalizácie údajov. Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Zásada obmedzenia účelu tak bráni prevádzkovateľovi využívať získané údaje na akékoľvek spracovateľské operácie. Na druhej strane dáta, ktoré už boli zhromaždené, môžu byť skutočne užitočné na iné účely, ktoré neboli pôvodne špecifikované. Umožňuje sa preto nové, ďalšie využitie osobných údajov za predpokladu, že

- a) osobné údaje sú spracúvané na tzv. *privilegované účely*, t. j. účely archivácie, na vedecké účely, na účely historického výskumu a na štatistické účely a sú dodržané primerané záruky ochrany práv dotknutej osoby;⁴⁵
- b) sa dosiahol pozitívny výsledok *testu zlučiteľnosti*, t. j. spracúvanie osobných údajov získaných na ďalší, než pôvodne vymedzený účel je možné, ak tento ďalší účel úzko súvisí s pôvodným účelom spracúvania a je s ním zlučiteľný.

V prípade ďalšieho spracúvania osobných údajov na privilegované účely, alebo v prípade ďalšieho spracúvania osobných údajov na základe pozitívneho výsledku testu zlučiteľnosti sa už nevyžaduje žiadny iný samostatný právny základ, než je právny základ, ktorý umožňoval získavanie osobných údajov. Mení sa len pôvodný účel spracúvania osobných údajov, právny základ ostáva zachovaný. Vo vzťahu k dotknutej osobe, ak prevádzkovateľ zamýšľa spracúvať osobné údaje na ďalší účel ako ten, na ktorý boli získané, je povinný informovať dotknutú osobu o tomto ďalšom účele.

Test zlučiteľnosti

Test zlučiteľnosti predstavuje možnosť prevádzkovateľa spracúvať osobné údaje aj na ďalší účel, než na ktorý boli pôvodne získané, ak je ďalší účel zlučiteľný s pôvodným účelom spracúvania. Ak prevádzkovateľ zvažuje, či môže osobné údaje spracúvať aj na ďalší účel, než na ktorý boli pôvodne získané, je povinný zohľadniť tieto kritériá:

- a) akékoľvek prepojenie medzi účelmi, na ktoré sa osobné údaje pôvodne získali, a účelmi zamýšľaného ďalšieho spracúvania;
- b) okolnosti, za akých sa osobné údaje získali, najmä okolnosti týkajúce sa vzťahu medzi dotknutými osobami a prevádzkovateľom;
- c) povaha osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky;
- d) možné následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby;
- e) existencia primeraných záruk, ktoré môžu zahŕňať napríklad šifrovanie alebo pseudonymizáciu.

Zamestnávateľ prevádzkuje dopravu a jeho vodiči sa na začiatku, ale aj na konci každej pracovnej zmeny podrobujú dychovej skúške testujúcej prítomnosť alkoholu v krvi.

⁴⁵ Samotné ustanovenie § 7 druhá veta nového zákona o ochrane osobných údajov prezumuje, že ďalšie spracúvanie osobných údajov na tzv. privilegované účely, ak budú dodržané primerané záruky ochrany práv dotknutej osoby, sa považuje za zlučiteľné s pôvodným účelom spracúvania.

Zamestnávateľ zistil, že zhromaždené údaje z testovania vie využívať aj na kontrolu plnenia dochádzky a evidencie pracovného času dotknutých zamestnancov, a to navyše bez ich vedomia. Účel, ktorý zamestnávateľ sleduje týmto spracúvaním osobných údajov, je kontrola plnenia základných pracovných povinností zamestnancov v zmysle § 81 Zákonníka práce. Citované ustanovenie, okrem iných povinností, zahŕňa aj implicitný zákaz požitia alkoholu na pracovisku, či explicitnú povinnosť byť na pracovisku na začiatku pracovného času a odchádzať z neho až po skončení pracovného času. Aj keď všeobecná spojitosť medzi účelmi spracúvania tu existuje („kontrola plnenia základných povinností zamestnanca“), nemyslíme, že pri zohľadnení vyššie uvedených kritérií by zamestnávateľ dospel k pozitívnemu výsledku testu zlučiteľnosti. Signálov, že použitie údajov získaných z testovania na alkohol je nezlučiteľné s ďalším účelom evidovanie pracovného času a dochádzky, je viacero. Zamestnanec nemohol reálne očakávať takýto ďalší účel spracúvania, ďalší účel spracúvania má na neho potenciálny negatívny vplyv (vyvodzovanie disciplinárnych opatrení za neskoré príchody na pracovisko), spracúvajú sa údaje s citlivou povahou, medzi prevádzkovateľom a dotknutou osobou je nerovnováha vyplývajúca zo samotnej existencie pracovnoprávneho vzťahu a problém je aj v identifikovaní primeraných záruk (napríklad informovanie zamestnanca o ďalšom účele okrem kontroly limitov alkoholu). Ďalším príkladom nezlučiteľnosti účelov, ktorý možno uviesť, je situácia, ak zamestnávateľ v prevádzke z bezpečnostných dôvodov nainštaluje kamery a v tomto duchu informuje o tom svojich zamestnancov. S pôvodným účelom (bezpečnosť, ochrana majetku zamestnávateľa) je nezlučiteľný ďalší účel, a to využívanie monitorovania zamestnancov na účely plnenia ich pracovných povinností.

Uvedené kritériá pre posúdenie zlučiteľnosti účelov spracúvania osobných údajov sú uvádzané za slovným spojením „okrem iného“, čo znamená, že pre účely testu zlučiteľnosti je možné zvážiť aj ďalšie vhodné kritériá.

Test zlučiteľnosti nemusí prevádzkovateľ vykonať vtedy, ak dotknutá osoba vyjadrila svoj súhlas s ďalším účelom spracúvania svojich osobných údajov, alebo je spracúvanie osobných údajov na ďalší účel založené na právnom základe, ktorým je osobitný právny predpis. Zamestnávateľ napríklad získava a uchováva životopisy úspešných uchádzačov o zamestnanie v ich osobných spisoch. Okrem iných údajov, obsahujú životopisy aj údaj o dosiahnutom vzdelaní a počte rokov odbornej praxe. Pôvodným účelom získavania týchto údajov je výber a prijatie čo najvhodnejšieho kandidáta na obsadzovanú pracovnú pozíciu. Zamestnávateľ však zamýšľa využívať údaj o dosiahnutom vzdelaní a počte rokov dosiahnutej praxe aj na ďalší účel, a to na účel kariérneho postupu zamestnancov a vnútornej mobility pri obsadzovaní uvoľnených pracovných miest v rámci podniku. Ak si zamestnávateľ nie je istý výsledkom testu zlučiteľnosti pôvodného a ďalšieho účelu spracúvania osobného údajov, je v jeho záujme, aby dotknutú osobu požiadal o súhlas so spracúvaním aj na ďalší účel, ktorý zamýšľa.

Vyššie identifikované podmienky prípustnosti spracúvania získaných osobných údajov na ďalšie účely sa vzťahujú iba na pôvodného prevádzkovateľa. Ak by spracovateľskou operáciou malo dôjsť k preneseniu osobných údajov inému prevádzkovateľovi,

tento by musel disponovať vlastným právnym základom na takéto spracúvanie i „vlastnými“ výsledkami testu zlučiteľnosti.

Dosiahnutie sledovaného účelu znamená koniec oprávnenia spracúvania osobných údajov v takej forme, v akej je ich možné priradiť ku konkrétnej fyzickej osobe. Ide o vyjadrenie zásady minimalizácie uchovávaní údajov. Osobné údaje sa môžu uchovávať dlhšie, len ak sa majú spracúvať výlučne na privilegované účely a sú dodržané primerané záruky ochrany práv dotknutej osoby.

2.3.2 Zákonnosť spracúvania

K tomu, aby mohol prevádzkovateľ zákonným spôsobom spracúvať osobné údaje dotknutých osôb, musí mať tzv. **zákonné** oprávnenie, resp. relevantný právny základ. Každý účel spracúvania musí mať svoj **právny základ** s výnimkou situácie, ak je pôvodný účel zlučiteľný s ďalším účelom spracúvania (viď vyššie *test zlučiteľnosti*). Prevádzkovateľ je oprávnený spracúvať osobné údaje dotknutých osôb, pretože s tým dotknutá osoba súhlasí, alebo jej to dovoľuje iná zákonom presne stanovená skutočnosť. Nový zákon o ochrane osobných údajov v súlade s GDPR taxatívne stanovuje a mení okruh právnych základov spracúvania. V porovnaní so starým zákonom o ochrane osobných údajov zostávajú niektoré právne základy zachované, iné budú zrušené. Definícia súhlasu so spracúvaním osobných údajov sa v podstate nemenila, ale k jeho vyjadreniu pribudlo viacero ďalších podmienok.

Aktuálnou úlohou prevádzkovateľa je tak odkontrolovať právne základy spracúvania osobných údajov dotknutých osôb a zabezpečiť, aby tieto boli aktuálne a súladné s GDPR. Ak prevádzkovateľ zistí, že spracúva osobné údaje dotknutých osôb na niektorom právnom základe, ktorý bude zrušený, bude musieť nájsť a disponovať iným primeraným právnym základom. **Zrušia sa** tieto právne základy spracúvania osobných údajov:

- priamy marketing v poštovom styku (§ 10 ods. 3 písm. d) starého zákona o ochrane osobných údajov);
- ďalšie spracúvanie už zverejnených osobných údajov (§ 10 ods. 3 písm. e) starého zákona o ochrane osobných údajov);
- spracúvanie biometrických údajov, ak je nevyhnutné na plnenie zmluvy podľa § 10 ods. 3 pís. b), alebo ak je nevyhnutné na ochranu práv a právom chránených záujmov podľa § 10 ods. 3 písm. g) (§ 13 ods. 5 písm. c) a d) starého zákona o ochrane osobných údajov);
- jednorazový vstup (§ 15 ods. 4 starého zákona o ochrane osobných údajov);
- získavanie osobných údajov ich kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií (§ 15 ods. 6 starého zákona o ochrane osobných údajov);
- monitorovanie priestorov prístupných verejnosti (§ 15 ods. 7 starého zákona o ochrane osobných údajov).

Mnohí zamestnávateľia majú ošetrový vstup verejnosti do svojich budov cez právny základ podľa ust. § 15 ods. 4 starého zákona o ochrane osobných údajov v tzv. knihe návštev. V zmysle citovaného ustanovenia prevádzkovateľ, ktorý získava osobné údaje na účely identifikácie fyzickej osoby pri jej jednorazovom vstupe do jeho priestorov, je oprávnený od nej požadovať: meno, priezvisko, titul, číslo občianskeho preukazu alebo číslo služobného preukazu, alebo číslo cestovného dokladu, štátnu príslušnosť a preukázanie pravdivosti poskytnutých osobných údajov predkladaným dokladom. Vzhľadom na to, že uvádzaný právny základ bude zrušený, zamestnávateľ musí disponovať pri spracúvaní osobných údajov osôb vstupujúcich do jeho budov iným právnym základom. Využitelný je v tomto prípade právny základ „*oprávnený záujem prevádzkovateľa*“ (viď nižšie druhy právnych základov). Namíste je aj prehodnotenie zoznamu osobných údajov spracúvaných pri jednorazovom vstupe do budov, keďže nový zákon o ochrane osobných údajov už explicitne neustanovuje zoznam údajov, ktoré je možné spracúvať. V súlade so zásadou minimalizácie údajov nevidíme potrebu ani primeranosť spracúvania štátnej príslušnosti osôb vstupujúcich do budov rôznych súkromných zamestnávateľov.

2.3.2.1 Druhy právnych základov pri spracúvaní všeobecných osobných údajov

Podľa § 13 nového zákona o ochrane osobných údajov môže prevádzkovateľ osobné údaje dotknutých osôb spracúvať na základe aspoň jedného z týchto právnych základov:

- a) súhlas dotknutej osoby;
- b) spracúvanie na účely plnenia zmluvy;
- c) spracúvanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy;
- d) spracúvanie nevyhnutné na ochranu života, zdravia alebo majetku dotknutej osoby, alebo inej fyzickej osoby;
- e) spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- f) spracúvanie nevyhnutné na účel oprávneného záujmu.

Za najviac využiteľné v pracovnoprávných vzťahoch považujeme právne základy uvedené v písm. a) až c) a písm. f).

Mimo ustanovenia § 13 nového zákona o ochrane osobných údajov sú v ustanovení § 78 nového zákona o ochrane osobných údajov vyjadrené ďalšie osobitné právne základy spracúvania osobných údajov dotknutej osoby. Prevádzkovateľ je oprávnený spracúvať osobné údaje bez súhlasu dotknutej osoby aj vtedy, ak spracúvanie osobných údajov je nevyhnutné

- a) na akademický, umelecký, alebo literárny účel;
- b) pre potreby informovania verejnosti masovokomunikačnými prostriedkami a ak osobné údaje spracúva prevádzkovateľ, ktorému to vyplýva z predmetu činnosti;

- c) na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel pri prijatí primeraných záruk pre práva a slobody dotknutej osoby (tzv. privilegované účely);

Na tieto účely prevádzkovateľ nesmie spracúvať osobné údaje dotknutej osoby bez jej súhlasu, ak spracúvaním osobných údajov porušuje právo dotknutej osoby na ochranu jej osobnosti, alebo právo na ochranu súkromia, alebo takéto spracúvanie osobných údajov bez súhlasu dotknutej osoby vylučuje osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná.

Súhlas dotknutej osoby

Prevádzkovateľ je oprávnený spracúvať osobné údaje dotknutej osoby, ak dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel. Súhlas sa potom bude vzťahovať na všetky spracovateľské činnosti vykonávané na ten istý účel, alebo príbuzné a navzájom si blízke účely (*viď vyššie test zlučiteľnosti*). Súhlas môže byť daný aj na viacero výslovne uvedených účelov, ale takým spôsobom, aby dotknutá osoba mala možnosť samostatne prejavíť svoju slobodnú vôľu pre každý jednotlivý účel uvedený v súhlase.

GDPR prináša nové požiadavky bližšie určujúce obsahové a formálne podmienky súhlasu. Ide o jednostranný prejav vôle dotknutej osoby, ktorý má byť slobodne daný, informovaný, konkrétny, jednoznačný a odlišiteľný od iných vyhlásení. Osobitne sa pokazuje na slobodu súhlasu v pracovnoprávných vzťahoch, kde nepomer medzi zmluvnými stranami ohrozuje skutočne slobodné vyjadrenia súhlasu zo strany zamestnanca. Súhlas zapracovaný do pracovnej zmluvy indikuje nemožnosť zamestnanca udelenie súhlasu odmietnuť. Ideálne je súhlas so spracúvaním osobných údajov naformulovať na samostatnej listine popri pracovnej zmluve⁴⁶ s uistením, že odmietnutie alebo odvolanie súhlasu nebude zamestnávateľom v nijakom smere postihované. Ak sa zamestnávateľ predsa len súhlas so spracúvaním osobných údajov rozhodne zapracovať do pracovnej zmluvy, minimálne nech tak urobí v samostatnom článku/ustanovení pracovnej zmluvy. Súhlas so spracúvaním osobných údajov má byť jasne a zreteľne odlišný od iných skutočností (častí daného dokumentu), aby sa zabránilo tomu, že ho dotknutá osoba nejakým spôsobom prehliadne. Z hľadiska formulácie je potrebné upriamiť pozornosť na to, aby bol súhlas vyjadrený jasne, v zrozumiteľnej a ľahko dostupnej forme.

Prevádzkovateľ musí vedieť hodnoverne a kedykoľvek preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov. Je potrebné na to pamätať pri voľbe formy udelenia súhlasu a uchovávať (prípadne archivovať) získaný súhlas po celú dobu spracúvania osobných údajov.⁴⁷ Zákon výslovne formu udelenia súhlasu neurčuje,

46 Podmienky a náležitosti vyjadrenia súhlasu upravuje ust. § 15 nového zákona o ochrane osobných údajov. K tomu aj: MERRELL, L. EU General Data Protection Regulation – The impact on employers. Dostupné na internete: http://www.clarkslegal.com/Blog/Post_EU_General_Data_Protection_Regulation_The_impact_on_employers. [online] [cit. 15. 09. 2017].

47 Nesplnenie povinnosti preukázať existenciu poskytnutého súhlasu zamestnancom v situácii, kedy

je na zvážení prevádzkovateľa, čo si zvolí (písomná forma potvrdená vlastnoručným podpisom alebo zaručeným elektronickým podpisom, jednoduchá elektronická forma v podobe emailu, telefonická nahrávka, ústny súhlas vyjadrený pri osobnom stretnutí, označenie políčka pri návšteve internetového webového sídla, iné konkludentné správanie a pod.). Mlčanie, vopred označené políčka alebo nečinnosť dotknutej osoby sa za súhlas nepovažujú, pretože nie sú založené na aktívnom prístupe dotknutej osoby vyjadrujúcej súhlas so spracúvaním osobných údajov. Za vyjadrenie súhlasu je možné považovať aj také konanie, ak uchádzač o zamestnanie zašle životopis uchádzajúc sa o pracovnú ponuku, ak zamestnanec zašle/zverejní sám svoju fotografiu v intranetovej sieti využívanej vo firme a pod.

Nový zákon o ochrane osobných údajov nepreberá ustanovenie § 11 ods. 4 starého zákona, podľa ktorého mal obligatórne súhlas obsahovať údaj o tom, kto súhlas udeľuje; komu sa súhlas udeľuje; na aký účel sa súhlas udeľuje; zoznam alebo rozsah osobných údajov, ktoré majú byť predmetom spracúvania; a čas platnosti súhlasu. Podľa recitálu 42 GDPR, ak dotknutá osoba udeľuje súhlas, mala by si byť vedomá, v akom rozsahu ho udeľuje, a aby sa zaistilo, že súhlas bude informovaný, dotknutá osoba si má byť vedomá aspoň identity prevádzkovateľa a zamýšľaných účelov spracúvania osobných údajov. Z udeleného súhlasu by tak malo byť naďalej zrejmé, kto súhlas udelil, komu ho udelil, kedy bol súhlas udelený, aké informácie dostala dotknutá osoba pred udelením súhlasu a akým spôsobom bol súhlas udelený. Pozornosť je potrebné upriamiť na inovovanú informačnú povinnosť, ktorá má predchádzať získaniu súhlasu. GDPR a nový zákon o ochrane osobných údajov rozširujú informačné povinnosti pri získavaní osobných údajov, napr. o povinnosť informovať dotknutú osobu už aj o právnych základoch spracúvania, o dobe uchovávania osobných údajov, resp. o kritériách na jej určenie, ak dobu nie je možné určiť a pod. (bližšie viď právo na informácie, kapitola 3.3.1.). Informačná povinnosť môže, ale nemusí byť zapracovaná v súhlase. Prevádzkovateľ je ten, kto nesie dôkazné bremeno o plnení tejto povinnosti.

Všetky doteraz získané súhlasy budú platné len za predpokladu, že spĺňajú požiadavky GDPR a nového zákona o ochrane osobných údajov. V opačnom prípade bude potrebné, aby si prevádzkovatelia vyžiadali nové súhlasy, alebo zvolili iný právny základ spracúvania osobných údajov. Ak porovnáme obsahové náležitosti súhlasu podľa starej a novej právnej úpravy, možno dospieť k záveru, že pokiaľ súhlas dotknutej osoby splnil všetky náležitosti vyžadované starou právnou úpravou, bude takto udelený súhlas súladný aj s novou právnou úpravou (navyše bude len čas platnosti súhlasu). Pozor však na inovovanú informačnú povinnosť a zdôraznenie práva dotknutej osoby na odvolanie súhlasu. Tak jednoducho, ako možno súhlas udeliť, musí existovať rovnako jednoduchá možnosť dotknutej osoby, odvolať súhlas. O tejto možnosti musí byť dotknutá osoba vopred informovaná.

ho zamestnávateľ v zmysle právneho poriadku potrebuje pre spracúvanie osobných údajov, možno považovať za porušenie príslušného zákona s predpokladom nedovoleného spracúvania osobných údajov s ohľadom na chýbajúci právny základ.

K využívaniu súhlasu, ako právneho základu pre spracúvanie osobných údajov, si dovoľíme ešte jednu poznámku. Všeobecné povedomie o pravidlách ochrany osobných údajov je v praxi založené na tom, že súhlas dotknutej osoby „posväti“ akékoľvek narábanie s jej osobnými údajmi. Zaužívanou praxou našich zamestnávateľov je vkladať do pracovných zmlúv/dohôd osobitné články, vyjadrujúce takýto súhlas, niekedy všeobecný, niekedy viac špecifikovaný.⁴⁸ Problém akéhokoľvek spracúvania osobných údajov zamestnancov je podľa nich vyriešený tým, že dotknutá osoba vyjadrí súhlas so spracovateľskou operáciou. Sme toho názoru, že ani súhlas dotknutej osoby nemôže prelomiť zásadu minimalizácie údajov, v zmysle ktorej je *spracúvanie osobných údajov obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa osobné údaje spracúvajú*. Spracúvanie toho-ktorého konkrétneho osobného údaju musí byť nevyhnutné na dosiahnutie daného účelu spracúvania pri ktoromkoľvek právnom základe spracúvania, aj pri súhlase. Navyše Úrad v nejednom svojom rozhodnutí pri uložení sankcií vyčíta prevádzkovateľom vyžadovanie súhlasu od dotknutej osoby tam, kde ho vôbec nie je treba. Upozorňuje na to, že kombináciou dvoch právnych základov spracúvania osobných údajov postupujú prevádzkovatelia v rozpore s právnym režimom spracúvania osobných údajov. Obdobie po účinnosti GDPR a nového zákona o ochrane osobných údajov si pravdepodobne vyžiada prehodnotenie stanoviska Úradu. Podľa čl. 6 ods. 1 GDPR a v nadväznosti naň podľa ust. § 13 ods. 1 nového zákona o ochrane osobných údajov je spracúvanie zákonné iba vtedy a iba v tom rozsahu, keď sa vykonáva **aspoň na základe jedného z právnych základov** spracúvania vymenovaných v tomto ustanovení. Explicitne sa vyjadruje možná kumulácia viacerých právnych základov a nevylučuje sa tak postup prevádzkovateľa, keď si potvrdí spracúvanie osobných údajov súhlasom „pre istotu“, aj keď súhlas nepotrebuje.⁴⁹ Domnievame sa, že Úrad nebude môcť prevádzkovateľom vyčítať nezákonnosť postupu, ak použijú súhlas v kombinácii s ďalším právnym základom. Zároveň však vyjadrujeme svoje presvedčenie, že zamestnávatelia by mali spracúvanie osobných údajov naviazať na súhlas dotknutej osoby naozaj len vtedy, ak tu neexistuje iný právny základ, a keď sú v pozícii, keď si sami nie sú istí, či potrebujú súhlas dotknutej osoby. Takáto situácia nehrozí, ak spracúvajú osobné údaje svojich zamestnancov v dôsledku plnenia povinnosti uloženej právnym predpisom. Spracúvaním osobných údajov na základe súhlasu dotknutej osoby sa navyše vystavujú zmätočným situáciám, keď sa dotknutá osoba bude domáhať takej právnej

48 Napríklad: „Zamestnanec podpisom tejto zmluvy výslovne vyjadruje svoj súhlas s použitím svojich osobných údajov v súlade so zákonom č. 122/2013Z. z. o ochrane osobných údajov v znení neskorších predpisov pre účely prác a povinností z pracovnoprávných vzťahov založených pracovnou zmluvou a pre účely plnenia povinností zamestnanca a zamestnávateľa z poistenia v zmysle zákona č. 580/1994 Z. z. o zdravotnom poistení v znení neskorších predpisov, zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov a zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov.“ Dostupné na internete: <http://www.profesia.sk/kariera-v-kocke/vzory-dokumentov/vzor-pracovnej-zmluvy/>. [online]. [cit. 15.09.2017].

49 Porovnaj: VOJTKO, J. Automatizované rozhodovanie a profilovanie v pracovnoprávných vzťahoch podľa Všeobecného nariadenia o ochrane údajov. In: Časopis pro právní vědu a praxi, XXV, 2/2017, s. 255–274. Dostupné na internete: <https://doi.org/10.5817/CPVP2017-2-5>. [online] [cit. 15. 09. 2017].

ochrany, ktorú zákon o ochrane osobných údajov priznáva vo vzťahu k spracúvaniu osobných údajov na základe súhlasu,⁵⁰ najmä práva súhlas kedykoľvek odvolať. Tu len upozorňujeme, že odvolanie súhlasu nemusí vždy pre prevádzkovateľa predstavovať aj povinnosť zlikvidovať osobné údaje, keďže súhlas bol daný k určitým účelom. Po odvolaní súhlasu je prevádzkovateľ povinný prestať spracúvať osobné údaje pre ten účel, ku ktorému bol súhlas udelený a následne odvolaný. Rovnako v prípade, že prevádzkovateľ použil súhlas pre prípady, keď spracúvaniu osobných údajov svedčí iný právny dôvod (predovšetkým spracúvanie na základe zákona), neznamená odvolanie súhlasu (teda úkonu, ktorý nebol nevyhnutný pre spracúvanie) povinnosť prevádzkovateľa prestať spracúvať, či zlikvidovať spracúvané osobné údaje (pozri k tomu aj kapitolu 3.3.4. Právo na vymazanie).

Spracúvanie na účely plnenia zmluvy

Prevádzkovateľ je oprávnený spracúvať osobné údaje bez súhlasu dotknutej osoby vtedy, ak je spracúvanie nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby. Dotknutá osoba je zmluvnou stranou, iniciátorom zmluvy alebo účastníkom predzmluvných vzťahov. Účelom spracúvania osobných údajov je v tomto prípade predmet zmluvy.

Spracúvanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy

Prevádzkovateľ je oprávnený spracúvať osobné údaje dotknutej osoby, ak je spracúvanie jej osobných údajov nevyhnutné podľa osobitného predpisu (minimálne s právnu silou zákona), alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Pri spracúvaní osobných údajov na základe osobitného predpisu, resp. medzinárodnej zmluvy, prevádzkovateľ spracúva osobné údaje o dotknutých osobách bez ich súhlasu (t. j. na spracúvanie ho oprávňuje a splnomocňuje priamo osobitný predpis, resp. medzinárodná zmluva). Pri spracúvaní osobných údajov na základe tohto právneho základu je prevádzkovateľ viazaný povinnosťou spracúvať osobné údaje len v rozsahu a spôsobom, ktorý tento osobitný predpis alebo medzinárodná zmluva ustanovuje. Prevádzkovateľ je teda oprávnený spracúvať len také osobné údaje, ktoré sú priamo vymedzené osobitným predpisom, alebo medzinárodnou zmluvou (uvádzaný zoznam osobných údajov), alebo také osobné údaje, ktoré sú nevyhnutné na dosiahnutie osobitným zákonom alebo medzinárodnou zmluvou stanoveného účelu (rozsah osobných údajov).⁵¹

Osobitný právny predpis je pomerne častým, ak nie najčastejším právnym základom spracúvania osobných údajov zamestnancov. Oprávnenie a podmienky spracúvania osobných údajov v pracovnoprávných vzťahoch upravujú osobitné zákony, primár-

50 VALENTOVÁ, T., ŠVEC, M. Ochrana osobných údajov v pracovnoprávných vzťahoch. Bratislava: Wolters Kluwer, 2016, s. 40. ISBN 978-80-8168-493-7.

51 Napr. čl. 11 Zákonníka práce (osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával).

ne Zákonník práce, ktorý prostredníctvom úpravy pracovnoprávných vzťahov definuje aj rozsah alebo zoznam osobných údajov, ktoré je pri jednotlivých úkonoch v pracovnoprávných vzťahoch možné spracúvať. Zákonník práce teda na účely pracovnoprávných vzťahov predstavuje osobitný predpis v zmysle § 13 písm. c) nového zákona o ochrane osobných údajov, ktorý oprávňuje prevádzkovateľa (zamestnávateľa) na účely spojené s pracovnoprávnym vzťahom, spracúvať osobné údaje. Rámcový účel spracúvania, zoznam alebo rozsah osobných údajov a druhy spracovateľských operácií zamestnávateľ okrem Zákonníka práce nájde v nasledujúcich právnych predpisoch (vždy v znení neskorších predpisov):

- zákone č. 55/2017 Z. z. o štátnej službe
- zákone č. 552/2003 Z. z. o výkone práce vo verejnom záujme
- zákone č. 553/2003 Z. z. o odmeňovaní niektorých zamestnancov pri výkone práce vo verejnom záujme a o zmene a doplnení niektorých zákonov
- zákone č. 595/2003 Z. z. o dani z príjmov
- zákone č. 461/2003 Z. z. o sociálnom poistení
- zákone č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov
- zákone č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov
- zákone č. 43/2004 Z. z. o starobnom dôchodkovom sporení
- zákone č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov
- zákone č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov
- zákone č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov a pod.

Zamestnávateľ sa potrebuje orientovať v osobitných právnych predpisoch, aby zbytočne a nad rámec nevyžadoval súhlas zamestnanca, keď ho nepotrebuje. Vyžadovanie súhlasu dotknutej osoby „*pre prípad..., keď získaním súhlasu, aj keď ho nepotrebujem, nič nepokazím*“, ako sme už uviedli nehodnotí Úrad vôbec pozitívne a už v nejednom rozhodnutí o uložení pokuty na to prevádzkovateľov upozornil. Na druhej strane je potrebné doplniť, že samotná orientácia v osobitných právnych predpisoch, využitelných ako právny základ spracúvania osobných údajov, nie je postačujúca. Právne predpisy je možné považovať za osobitný zákon, t. j. za právny základ spracúvania osobných údajov za predpokladu, že spĺňajú určité atribúty. Osobitný zákon má ustanovovať účel spracúvania osobných údajov, kategóriu dotknutých osôb a zoznam spracúvaných osobných údajov, alebo rozsah spracúvaných osobných údajov. Pre právne akceptovanie zákona, ako právneho základu pre spracúvanie osobných údajov, je nevyhnutné splnenie všetkých podmienok kumulatívne, t. j. súčasne v okamihu jeho požiadavky na jeho praktické použitie. Mnohé, zamestnávateľmi použiteľné právne predpisy, tieto atribúty spĺňajú

implicitne, preto ich využitie, ako právnych základov, bude vyžadovať aj určité znalosti interpretácie.

Osobitný prípad právneho základu spracúvania osobných údajov na základe právneho predpisu je pre zamestnávateľov vyjadrený v ustanovení § 78 ods. 3 nového zákona o ochrane osobných údajov. Podľa citovaného ustanovenia „*prevádzkovateľ, ktorý je zamestnávateľom dotknutej osoby, je oprávnený poskytovať jej osobné údaje alebo zverejniť jej osobné údaje v rozsahu titul, meno, priezvisko, pracovné zaradenie, služobné zaradenie, funkčné zaradenie, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresu elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa, ak je to potrebné v súvislosti s plnením pracovných povinností, služobných povinností alebo funkčných povinností dotknutej osoby. Poskytovanie osobných údajov alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.*“ Na spracúvanie osobných údajov zamestnanca, uvedených v ust. § 79 ods. 3 nového zákona o ochrane osobných údajov, zamestnávateľ nepotrebuje súhlas zamestnanca, pretože právnym základom spracúvania je priamo zákon o ochrane osobných údajov. Predpokladom zákonného spracúvania uvedených osobných údajov zamestnanca je, že zamestnávateľ dodrží stanovený účel. A to, ak je poskytnutie alebo zverejnenie osobných údajov potrebné v súvislosti s plnením pracovných, služobných alebo funkčných povinností dotknutej osoby. V porovnaní so starým zákonom o ochrane osobných údajov pribudla do nového zákona o ochrane osobných údajov možnosť bez súhlasu zamestnanca poskytovať a zverejňovať aj jeho osobné alebo zamestnanecké číslo. Aj keď sa pôvodne uvažovalo, že medzi zoznam osobných údajov uvedených v § 78 ods. 2 nového zákona o ochrane osobných údajov bude zaradená aj fotografia zamestnanca, od tohto úmyslu sa upustilo. Na zverejnenie fotografie zamestnanca, napr. na svojom webovom sídle pre účely identifikácie okruhu aktuálne zamestnávaných fyzických osôb, tak zamestnávateľ potrebuje súhlas zamestnanca (bližšie kapitola 4.8.).

Spracúvanie nevyhnutné na účel oprávneného záujmu

Spracúvanie osobných údajov dotknutej osoby je možné bez jej súhlasu, ak je spracúvanie nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany, ktorý sa takýmto spracúvaním sleduje. O oprávnený záujem, ako právny základ spracúvania osobných údajov, ide v tom prípade, ak medzi dotknutou osobou a prevádzkovateľom už existuje vzťah, napríklad pracovnoprávny vzťah. Oprávnený záujem prevádzkovateľa alebo tretej strany však nesmie prevažovať nad záujmami alebo právami dotknutej osoby. Pri využívaní tohto právneho základu má byť prevádzkovateľ schopný preukázať, akým spôsobom sa vysporiadal s posúdením vyváženosti ním sledovaných oprávnených záujmov a práv a slobôd dotknutých osôb. Ak v danom čase a kontexte spracúvania dotknutá osoba vôbec neočakáva spracúvanie, alebo neočakáva ďalšie spracúvanie jej osobných údajov, pravdepodobne oprávnený záujem prevádzkovateľa prevažuje nad záujmami a právami dotknutej osoby.

Využitie tohto právneho základu zaťažuje prevádzkovateľa osobitnou povinnosťou výslovne upozorniť dotknutú osobu na jej právo namietat takéto spracúvanie (bližšie viď kapitola 3.3.7) najneskôr pri prvej komunikácii s ňou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií.

Oprávneným záujmom zamestnávateľa, ktorý má pobočky roztrúsené po celom Slovensku, je tak napríklad vnútorný prenos osobných údajov zamestnancov medzi jednotlivými pobočkami, najmä na účely rôznej administrácie týkajúcej sa existujúcich pracovnoprávných vzťahov. Na takéto spracúvanie osobných údajov (prenos) zamestnávateľ nepotrebuje súhlas zamestnanca, právnym základom je oprávnený záujem prevádzkovateľa, ktorý však nesmie zabudnúť na primeranú bezpečnosť tejto spracovateľskej operácie (k spracúvaniu osobných údajov zamestnanca na právnom základe „oprávneného záujmu“ zamestnávateľa pozri aj kapitoly 4.9. až 4.11.).

2.3.2.2 Druhy právnych základov pri spracúvaní citlivých osobných údajov

Ako sme uviedli, vo všeobecnosti sa zakazuje spracúvanie citlivých osobných údajov, pretože, ak by došlo k zneužitiu týchto údajov, mohlo by to pre dotknutú osobu predstavovať výraznejší zásah do jej základných práv a slobôd. Zákaz spracúvania citlivých osobných údajov je prelomený taxatívne stanoveným zoznamom právnych základov, na základe ktorých možno citlivé osobné údaje spracúvať. Tento zoznam jedenástich právnych základov spracúvania citlivých osobných údajov je uvedený v čl. 9 ods. 2 GDPR a ust. § 16 ods. 2 nového zákona o ochrane osobných údajov a zahŕňa spravidla špecifické situácie spracúvania týchto dát. Vyberáme tie, ktoré majú priamu relevanciu v oblasti pracovnoprávných vzťahov. Spracúvanie citlivých osobných údajov zamestnanca je možné na základe:

a) výslovného súhlasu dotknutej osoby;

Kým spracúvanie všeobecných osobných údajov je možné na právnom základe súhlasu dotknutej osoby, spracúvanie citlivých osobných údajov vyžaduje *výslovný* súhlas dotknutej osoby. Výslovný súhlas je potrebné chápať ako vyjadrený súhlas. Požiadavka výslovného súhlasu teda znamená, že súhlas nie je vyvođený. Napríklad situácia, v ktorej zamestnávateľ informuje zamestnanca, že jeho zdravotné záznamy prenesie spoločnosť poskytujúcej zdravé výživové doplnky na účely zasielania marketingových správ, pokiaľ nevznesie námietku (napr. e-mailom na adresu personalistiky), nespĺní požiadavku výslovného súhlasu. Rovnako tak sa výslovný súhlas vyžaduje na spracúvanie rodného čísla,⁵² ak sa spracúva na právnom základe súhlasu (ust. § 79 ods. 4 nového zákona o ochrane osobných údajov). Samotný podpis pracovnej zmluvy, v ktorej je uvedené rodné číslo zamestnanca, vlastnosť výslovného súhlasu nespĺňa. Tradične sa výslovný súhlas udeľuje písomne alebo elektronicky. Nevylučuje sa ani ústne poskytnutie výslovného súhlasu, avšak dokázať poskytnutie takéhoto súhlasu môže byť pre prevádzkovateľa skutočne ťažké. Z hľadiska obsahu musí byť v naformulovanom súhlase uvedený

52 Rodné číslo už nepatrí k citlivým osobným údajom. Bližšie kapitola 5.3.

konkrétny citlivý osobný údaj, s ktorého spracúvaním má dotknutá osoba súhlasiť. Ani výslovný súhlas dotknutej osoby so spracúvaním jej osobných údajov však neprelomí situáciu, ak poskytnutie súhlasu vylučuje osobitný predpis.

b) spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia ... podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby;

Na tomto právnom základe je možné spracúvať citlivé osobné údaje zamestnanca bez jeho súhlasu, ako napríklad výsledky posúdenia zdravotnej alebo psychickej spôsobilosti na prácu. Informáciu o tom, či je/nie je zamestnanec zdravotne alebo psychicky spôsobilý na výkon práce, umožňuje zamestnávateľovi v tomto rozsahu spracúvať § 41 ods. 2 Zákonníka práce. Subjekt, ktorý vykonáva posúdenie zdravotnej, či psychickej spôsobilosti na výkon práce, či iné posúdenia v rámci preventívneho pracovného lekárstva, disponuje samostatným právnym základom spracúvania citlivých osobných údajov dotknutých osôb uvedenom v ust. § 16 ods. 2 písm. h) nového zákona o ochrane osobných údajov.

Ďalšie osobitné zákony umožňujú zamestnávateľovi spracúvať aj osobitnú kategóriu osobných údajov o porušení ustanovení zakladajúcich trestnú zodpovednosť, alebo administratívnoprávnu zodpovednosť v rozsahu uvedenom na výpise/odpise z registra trestov, ak ide o prácu, pri ktorej sa podľa osobitného predpisu vyžaduje bezúhonnosť.⁵³

c) spracúvanie vykonáva v rámci oprávnenej činnosti odborová organizácia;

Spracúvanie citlivých osobných údajov odborovou organizáciou bude zákonné za kumulatívneho naplnenia nasledujúcich podmienok. Toto spracúvanie:

- sa týka iba jej členov alebo tých fyzických osôb, ktoré sú s odborovou organizáciou vzhľadom na ich ciele v pravidelnom styku,
- slúži výlučne pre jej vnútornú potrebu a
- údaje nebudú poskytnuté tretej strane bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby.

d) spracúvanie je nevyhnutné na účely práva sociálneho zabezpečenia

Ide o prípady spracúvania citlivých údajov zamestnancov na účely sociálneho poistenia, poskytovania štátnych sociálnych dávok, či na ďalšie účely plnenia povinností alebo uplatnenia práv prevádzkovateľa zodpovedného za spracúvanie v oblasti pracovného práva a v oblasti služieb zamestnanosti, ak to prevádzkovateľovi vyplýva z osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

⁵³ Napríklad výkon práce v rámci súkromných bezpečnostných služieb v zmysle zákona č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti). Bližšie k bezúhonnosti zamestnanca pozri: BARINKOVÁ, M. Bezúhonnosť zamestnanca. In: Personálny a mzdový poradca podnikateľa. - ISSN 1335-1508. - Roč. 21, č. 9-10 (2015), s. 42-54.

Okrem právnych základov spracúvania citlivých osobných údajov uvedených v písm. a) až d), ktoré predstavujú najčastejšie právne základy spracúvania pre oblasť pracovnoprávnych vzťahov, nemožno vylúčiť, že zamestnávateľ spracúvanie citlivých údajov zamestnanca bez jeho súhlasu legitímne oprie aj o ďalšie špecifické situácie uvedené v čl. 9 ods. 2 GDPR a ust. § 16 ods. 2 nového zákona o ochrane osobných údajov. Zamestnávateľ nepotrebuje súhlas zamestnanca, ak spracúva také jeho citlivé osobné údaje, ktoré zamestnanec o sebe preukázateľne zverejnil; ktoré zamestnávateľ nevyhnutne potrebuje na uplatnenie právneho nároku, alebo pri výkone súdnej právomoci; a ktoré spracúva na tzv. *privilegované účely* (archivácia, vedecký účel, účel historického výskumu, štatistika).

Mimo citovaných ustanovení je osobitne upravený právny základ pre spracúvanie citlivých osobných údajov, ktorými sú genetické údaje, biometrické údaje a údaje týkajúce sa zdravia. Tieto tri kategórie citlivých osobných údajov je v súlade s § 79 ods. 5 nového zákona o ochrane osobných údajov možné bez súhlasu dotknutej osoby spracúvať **aj** na právnom základe osobitného predpisu⁵⁴ alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

54 V podmienkach Slovenskej republiky napríklad zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

III. Zamestnanec v pozícii dotknutej osoby

3.1 Dotknutá osoba

Zamestnanec je v kontexte aplikácie pravidiel ochrany osobných údajov **dotknutou osobou**, t. j. fyzickou osobou, ktorej osobné údaje sa spracúvajú. Nepodstatná je:

- i. *kvalifikácia pracovnoprávného vzťahu*: ochrana osobných údajov sa v rovnakom rozsahu vzťahuje na pracovný pomer založený pracovnou zmluvou, pracovno-právne vzťahy založené dohodami o prácach vykonávaných mimo pracovného pomeru, či faktický pracovný pomer.
- ii. *štátna príslušnosť*: právo na ochranu osobných údajov je univerzálnym právom, ktoré sa neobmedzuje na štátnych príslušníkov alebo obyvateľov určitej krajiny (ochrana osobných údajov sa vzťahuje na každú fyzickú osobu bez ohľadu na štátnu príslušnosť, či osobu bez štátnej príslušnosti).

Okrem zamestnanca prichádzajú do úvahy ako dotknuté osoby tiež uchádzači o zamestnanie, dočasne pridelení zamestnanci, bývalí zamestnanci, rodinní príslušníci zamestnanca, ak sa ich údaje spracúvajú v súvislosti s realizovanými pracovnoprávnymi vzťahmi a pod.

Podľa vyššie uvedeného poňatia by bolo možné považovať za osobné údaje iba údaje živých fyzických osôb. Smrťou fyzickej osoby v zmysle ust. § 7 Občianskeho zákonníka zaniká totiž spôsobilosť fyzickej osoby mať práva a povinnosti. Smrťou zamestnanca končí pracovnoprávny vzťah a pre zamestnávateľa, i samotného zosnulého zamestnanca, je hodnota jeho osobných údajov minimálna, ak vôbec nejaká. Taká však určite nie je pre pozostalých. GDPR sa podľa bodu 27 úvodných ustanovení skutočne neuplatňuje na osobné údaje zosnulých osôb. Členské štáty však môžu stanoviť pravidlá týkajúce sa spracúvania osobných údajov zosnulých osôb. Slovenská republika možnú odchýlku využila a nový zákon o ochrane osobných údajov v ust. § 78 ods. 7 **ponecháva v platnosti** ust. § 12 ods. 7 starého zákona o ochrane osobných údajov v zmysle ktorého: „*Ak dotknutá osoba nežije, súhlas vyžadovaný podľa tohto zákona alebo osobitného predpisu môže poskytnúť jej blízka osoba. Súhlas nie je platný, ak čo len jedna blízka osoba písomne vyslovila nesúhlas.*“ Osobné údaje zosnulého sú totiž spojené s osobnými údajmi žijúcich fyzických osôb, preto je akékoľvek svojvoľné nakladanie s osobnými údajmi zosnulého zamestnanca neprípustné, a napríklad na zverejnenie fotografie zamestnanca s dátumom narodenia i úmrtia za účelom uctenia si jeho pamiatky v podnikovom časopise, či na webovom sídle, by zamestnávateľ potreboval súhlas blízkej osoby.

Súčasne však nový zákon o ochrane osobných údajov nepreberá ust. § 28 ods. 9 starého zákona, podľa ktorého: „*Ak dotknutá osoba nežije, jej práva, ktoré mala podľa tohto zákona, si môže uplatniť blízka osoba.*“ V neprevzatí citovaného ustanovenia § 28 ods. 9 nevidíme problém, pretože týmto nie je dotknutá posmrtná ochrana osobnosti a súkromia (vrátane niektorých aspektov ochrany osobných údajov) podľa § 15 Občianskeho zákonníka v znení neskorších predpisov, podľa ktorého: „*Po smrti fyzickej*

osoby patrí uplatňovať právo na ochranu jej osobnosti manželovi a deťom, a ak ich niet, jeho rodičom.“

Vo vzťahu k opačnému garde, ak blízke osoby žiadajú zamestnávateľa o prístup k osobným údajom zosnulého, aj bez existencie explicitnej právnej úpravy je potrebné postupovať korektne a citlivo, a vyhovieť ich požiadavkám za predpokladu vierohodného preukázania ich postavenia k zosnulému zamestnancovi.

GDPR a ani vnútroštátny zákon o ochrane osobných údajov nechráni osobné údaje právnických osôb, ani fyzických osôb – živnostníkov (ďalej len podnikatelia). Prax však prináša aj prípady, kedy nie je možné oddeliť údaje o právnickej osobe od údajov o fyzických osobách, najmä, ak sa tieto osoby zúčastňujú na činnosti právnickej osoby. Typickým príkladom je vedenie obchodného registra, ktorý obsahuje osobné údaje konateľov v pozícii štatutárnych orgánov. Identifikačné údaje podnikateľov i osôb konajúcich v ich mene používané v bežnom obchodnom styku, ktorésú zverejnené v súlade so zákonom v príslušných registroch, nie sú osobnými údajmi. Ďalšie identifikátory, ktoré už majú súkromnú povahu, je ale potrebné považovať za osobné údaje, a teda aj takýto subjekt sa môže stať dotknutou osobou. V tejto súvislosti sa diskutuje, či vlastnoručný podpis konateľa obchodnej spoločnosti je, alebo nie je osobným údajom. Zo zverejneného vyjadrenia Úradu vyplýva, že aj na podpis štatutárneho orgánu, osoby oprávnenej konať za právnickú osobu, ako aj inej osoby (napr. kontaktnej osoby u zamestnávateľa) sa nahliada ako na osobný údaj. Uvedené sa vzťahuje aj na fyzickú osobu – podnikateľa (Vid' *Vyjadrenie k povinnému zverejňovaniu informácií podľa ustanovení § 5a a § 5b zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) z pohľadu ochrany osobných údajov*). Súhlasíme s citovaným vyjadrením Úradu, pretože spojením mena, priezviska a vyobrazenia vlastnoručného podpisu ide o charakteristiku, ktorou je identifikovateľná konkrétna fyzická osoba. Aj keď sa konateľ spoločnosti vlastnoručne podpísal pod obchodnú transakciu, ktorá sa nijako netýka jednotlivca, je pravdepodobné, že ďalšie spracúvanie takého údajja (napr. zverejnenie podpisu) je spôsobilé ohroziť práva a chránené záujmy, ktoré mu patria ako fyzickej osobe. Informácie o právnických osobách sa môžu na základe ich vecného obsahu pokladať za informácie „týkajúce sa“ fyzických osôb a za splnenia ďalších kritérií za osobné údaje. Okrem vlastnoručného podpisu konateľa za také možno považovať aj meno právnickej osoby odvodené od mena fyzickej osoby; podnikovú elektronickú poštu, ktorú využíva konkrétny zamestnanec; informácie o podniku, v ktorých je opísané správanie vlastníka, obchodné tajomstvo, či daňové tajomstvo, ktoré ako súbory viacerých informácií môžu obsahovať aj informácie o dotknutých osobách a pod.

3.2 Právna subjektivita dotknutej osoby

Spôsobilosť mať práva a povinnosti a spôsobilosť na právne úkony v súvislosti so spracúvaním osobných údajov sa riadi ustanoveniami Občianskeho zákonníka. Spôsobilosť fyzickej osoby mať práva a povinnosti patriace jej, ako dotknutej osobe podľa

zákona o ochrane osobných údajov, vzniká narodením a zaniká smrťou. Spôsobilosť na právne úkony vzniká priebežne v závislosti od rozumovej a vôľovej vyspelosti zodpovedajúcej veku maloletých a v plnom rozsahu vzniká plnoletosťou. Preto je v zásade aj maloletý spôsobilý dať súhlas so spracúvaním svojich osobných údajov.

GDPR prináša čiastkovú zmenu v tejto oblasti, pokiaľ ide o služby poskytované maloletým prostredníctvom internetu. Ak prevádzkovateľ spracúva osobné údaje dotknutej osoby na základe súhlasu dotknutej osoby, je spracúvanie osobných údajov maloletého zákonné, len ak má maloletý aspoň 16 rokov. Ak má maloletý menej ako 16 rokov, takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol, alebo schválil jeho zákonný zástupca. Uvedené podmienky sa nevzťahujú na off-line dáta, ani na osobné údaje spracúvané na inom právnom základe, než je súhlas.

Vyššie uvedené ustanovenie teda nemá vplyv na právnu subjektivitu mladistvého zamestnanca (15-18 rokov) a nevytvára žiadnu potrebnú interakciu zamestnávateľa a zákonného zástupcu na ochranu osobných údajov mladistvého v pracovnoprávných vzťahoch. Subjekt, ktorému je priznaná pracovnoprávna subjektivita, čo znamená, že je spôsobilý uvedomiť si práva a povinnosti z tohto záväzkového vzťahu, je spôsobilý uvedomiť si rovnako aj práva a povinnosti vyplývajúce mu z postavenia dotknutej osoby. Ak má zamestnávateľ pochybnosti, či mladistvý zamestnanec chápe všetky riziká, pravidlá a záruky súvisiace so spracúvaním osobných údajov, v záujme jeho ochrany **môže zväziť** kontaktovanie zákonných zástupcov mladistvého.

3.3. Práva dotknutej osoby

Práva dotknutej osoby sú dôležitým prvkom ochrany osobných údajov. Popri zamestnancovi a spotrebiteľovi je dotknutá osoba ďalším subjektom v slabšom postavení vo vzťahu k druhej strane. GDPR rozširuje a spresňuje jednotlivé práva dotknutých osôb s cieľom „vybalansovať“ nerovný vzťah dotknutej osoby a prevádzkovateľa. Dotknutej osobe patria tieto práva:

1. právo na informácie;
2. právo na prístup;
3. právo na opravu;
4. právo na vymazanie (právo „na zabudnutie“);
5. právo na obmedzenie spracúvania;
6. právo na prenosnosť osobných údajov;
7. právo namietat;
8. právo na neúčinnosť automatizovaného individuálneho rozhodovania, vrátane profilovania.

Z teoretického hľadiska možno právo na informácie zaradiť k pasívnym právam dotknutej osoby, t. j. prevádzkovateľ vyvíja aktivitu smerom k dotknutej osobe, aby jej poskytol, resp. sprístupnil zákonom vyžadovaný rozsah informácií. Práva dotknutej osoby

uvedené v bodoch 2 až 8 sú založené na aktívnom prístupe samotnej dotknutej osoby.

Vo vzťahu k zamestnávateľom a realizácii pracovnoprávných vzťahov neexistujú žiadne výnimky, ktoré by vylučovali možnosť zamestnanca uplatňovať si niektoré z vyššie uvedených práv.

3.3.1. Právo na informácie

Na účely zákona o ochrane osobných údajov sa rozumie súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, *informovaný* a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov (čl. 7 GDPR, ust. § 5 písm. a) nového zákona o ochrane osobných údajov).

Právne perfektný súhlas, okrem iných náležitostí, teda vyžaduje, aby pred prvou spracovateľskou operáciou (spravidla získavanie osobných údajov) bola dotknutá osoba informovaná o určitých skutočnostiach. Je potrebné si uvedomiť, že **súhlas so spracúvaním osobných údajov nie je zároveň splnením informačnej povinnosti prevádzkovateľa, ale splnenie informačnej povinnosti môže byť jeho súčasťou**. Je vecou každého prevádzkovateľa, aký spôsob hodnoverného splnenia informačnej povinnosti si zvolí. Ak má napríklad zamestnávateľ vo svojich podmienkach zavedený intranetový spôsob oboznamovania zamestnancov o všetkých aspektoch týkajúcich sa pracovnoprávných vzťahov, môže tento prostriedok zvoliť aj pre plnenie informačnej povinnosti. V predmetnom prípade si musí len zabezpečiť, aby na požiadanie dozorného orgánu (Úradu) vedel hodnoverne preukázať, že dotknutým osobám boli všetky relevantné informácie poskytnuté.

Plnením informačnej povinnosti prevádzkovateľa sa teda dotknutej osobe poskytuje možnosť, aby sa kvalifikovane rozhodla, či súhlas so spracúvaním osobných údajov poskytne, alebo neposkytne. Novinkou v porovnaní so starou právnou úpravou je plnenie tejto informačnej povinnosti aj vtedy, ak prevádzkovateľ získava osobné údaje priamo od dotknutej osoby na právnom základe osobitného právneho predpisu, či na základe medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. V plnej miere sa tak informačná povinnosť dotkne už aj zamestnávateľov, aj keď spracúvajú osobné údaje v pracovnoprávných vzťahoch v prevažnej miere na právnom základe osobitného zákona. Možno len odporúčať, aby do 25. mája 2018 zamestnávatelia vypracovali interný dokument obsahujúci komplexné splnenie informačnej povinnosti v celej obsahovej šírke vyžadovanej GDPR a novým zákonom o ochrane osobných údajov a po 25. máji 2018 s ním preukázateľne oboznámili všetkých svojich zamestnancov, resp. aj ďalšie dotknuté osoby. GDPR a nový zákon o ochrane osobných údajov umožňujú informácie, ktoré sa majú poskytnúť dotknutej osobe podľa čl. 13 a 14 GDPR, resp. § 19 a 20 nového zákona o ochrane osobných údajov, podať v kombinácii so štandardizovanými ikonami, s cieľom poskytnúť dobre viditeľný, jasný a zrozumiteľný prehľad zamýšľaného spracúvania osobných údajov. Štandardizované ikony musia byť strojovo čitateľné, ak sú použité v elektronickej podobe. Informácie, ktoré majú byť obsiahnuté v štandardizova-

ných ikonách a postupy určovania štandardizovaných ikon, ustanoví všeobecne záväzný právny predpis, ktorý vydá Úrad.

Zoznam informácií, ktoré sa majú poskytnúť, ak **sú** osobné údaje získané priamo od dotknutej osoby:

Tabuľka č. 1 Porovnanie novej (čl. 13 GDPR, ust. § 19 zákona) a starej právnej úpravy (ust. § 15 ods. 1 zákona)

podľa nového zákona o ochrane osobných údajov	podľa starého zákona o ochrane osobných údajov
identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol vymenovaný;
XXX	zoznam osobných údajov alebo rozsah osobných údajov;
kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	XXX
kontaktné údaje zodpovednej osoby, ak je určená;	XXX
účel spracúvania osobných údajov, na ktorý sú osobné údaje určené;	účel spracúvania osobných údajov;
právny základ spracúvania osobných údajov;	XXX
oprávnené záujmy prevádzkovateľa, ak sa osobné údaje spracúvajú na tomto právnom základe;	XXX
identifikácia príjemcu alebo kategória príjemcu, ak existuje; *	identifikačné údaje sprostredkovateľa; ak má prevádzkovateľ sprostredkovateľa; tretie strany, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje poskytnuté; okruh príjemcov, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje sprístupnené; preukázanie totožnosti oprávnenej osoby, ktorá získava osobné údaje, alebo preukázanie príslušnosti oprávnenej osoby hodnoverným dokladom k tomu subjektu, v mene ktorého koná;
* príjemcom je každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je tretou stranou; teda príjemcom je aj sprostredkovateľ; za príjemcu sa nepovažuje orgán verejnej moci, t. j. prevádzkovateľ nie je povinný informovať dotknutú osobu o tom, že poskytol jej osobné údaje orgánu verejnej moci;	
zamýšľaný prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, vrátane identifikácie krajiny alebo medzinárodnej organizácie a identifikácie tzv. primeraných záruk;	tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov;

ďalšie doplňujúce informácie pre dotknutú osobu:	ďalšie doplňujúce informácie pre dotknutú osobu:
doba uchovávaní osobných údajov; ak to nie je možné, informácie o kritériách jej určenia; (napr. po dobu jedného roka od zverejnenia, po dobu trvania pracovnoprávneho vzťahu);	čas platnosti súhlasu (vždy určitá doba, v rozpore so zákonom boli formulácie „až do odvolania súhlasu so spracúvaním osobných údajov“);
o práve požadovať od prevádzkovateľa prístup k jej osobným údajom;	poučenie o právach dotknutej osoby;
o práve na opravu jej osobných údajov;	poučenie o právach dotknutej osoby;
o práve na vymazanie jej osobných údajov alebo o práve na obmedzenie spracúvania jej osobných údajov;	poučenie o právach dotknutej osoby;
o práve namietat spracúvanie osobných údajov (vyžaduje sa výslovné upozornenie najneskôr pri prvej komunikácii s dotknutou osobou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií);	poučenie o právach dotknutej osoby;
o práve na prenosnosť osobných údajov;	poučenie o právach dotknutej osoby;
o práve kedykoľvek svoj súhlas odvolať;	poučenie o právach dotknutej osoby;
o práve podať návrh na začatie konania na Úrad;	poučenie o právach dotknutej osoby;
o tom, či je poskytovanie osobných údajov zákonnou požiadavkou, alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov;	poučenie o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje;
o existencii automatizovaného individuálneho rozhodovania, vrátane profilovania; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použití postupu, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osob- ných údajov pre dotknutú osobu;	XXX
XXX	formu zverejnenia, ak majú byť osobné údaje zverejnené.

Právna úprava ochrany osobných údajov vyžaduje iniciatívne konanie prevádzkovateľa pri plnení informačnej povinnosti. Informácie sa poskytujú pri získavaní osobných údajov, nie až na žiadosť dotknutej osoby. V prípade ak už dotknutá osoba niektorými informáciami disponuje (napríklad jej už boli skôr prevádzkovateľom poskytnuté), prevádzkovateľ nemusí informácie opätovne poskytovať, stačí poskytnúť len tie informácie, ktoré dotknutá osoba ešte nemá k dispozícii.

Zoznam informácií, ktoré sa majú poskytnúť, ak **nie sú** osobné údaje získané priamo od dotknutej osoby:

Tabuľka č. 2 Porovnanie novej (čl. 14 GDPR, ust. § 20 zákona) a starej právnej úpravy (ust. § 15 ods. 2 zákona)

podľa nového zákona o ochrane osobných údajov	podľa starého zákona o ochrane osobných údajov
identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol vymenovaný;
kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	XXX
kontaktné údaje zodpovednej osoby, ak je určená;	XXX
účel spracúvania osobných údajov, na ktorý sú osobné údaje určené;	účel spracúvania osobných údajov;
právny základ spracúvania osobných údajov;	XXX
kategórie spracúvaných osobných údajov;	zoznam osobných údajov;
oprávnené záujmy prevádzkovateľa, ak sa osobné údaje spracúvajú na tomto právnom základe;	XXX
identifikácia príjemcu alebo kategória príjemcu, ak existuje;	Identifikačné údaje sprostredkovateľa; ak prevádzkovateľ má sprostredkovateľa; tretie strany, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje poskytnuté; okruh príjemcov, ak sa predpokladá, alebo je zrejmé, že im budú osobné údaje sprístupnené;
zamýšľaný prenos osobných údajov do 3. krajiny alebo medzinárodnej organizácii, vrátane identifikácie 3. krajiny alebo medzinárodnej organizácie a identifikácie tzv. primeraných záruk;	Tretie krajiny, ak sa predpokladá, alebo je zrejmé, že sa do týchto krajín uskutoční prenos osobných údajov;

ďalšie doplňujúce informácie pre dotknutú osobu:	ďalšie doplňujúce informácie pre dotknutú osobu:
XXX	poučenie o možnosti rozhodnúť o spracúvaní získaných osobných údajov;
doba uchovávania osobných údajov, ak to nie je možné, informácie o kritériách jej určenia;	XXX
o práve požadovať od prevádzkovateľa prístup k jej osobným údajom;	poučenie o právach dotknutej osoby;
o práve na opravu jej osobných údajov;	poučenie o právach dotknutej osoby;
o práve na vymazanie jej osobných údajov, alebo o práve na obmedzenie spracúvania jej osobných údajov;	poučenie o právach dotknutej osoby;
o práve namietat spracúvanie osobných údajov (vyžaduje sa výslovné upozornenie najneskôr pri prvej komunikácii s dotknutou osobou, pričom informácia o tomto práve musí byť uvedená jasne a oddelene od akýchkoľvek iných informácií);	poučenie o právach dotknutej osoby;
o práve na prenosnosť osobných údajov;	poučenie o právach dotknutej osoby;
o práve kedykoľvek svoj súhlas odvolať;	poučenie o právach dotknutej osoby;
o práve podať návrh na začatie konania na Úrad;	poučenie o právach dotknutej osoby;
o zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov;	XXX
XXX	formu zverejnenia, ak majú byť osobné údaje zverejnené;
o existencii automatizovaného individuálneho rozhodovania, vrátane profilovania; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použítom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.	XXX

Zoznam informácií, ktoré sa majú poskytnúť, ak **nie sú** osobné údaje získané priamo od dotknutej osoby:

Tabuľka č. 3 Porovnanie zoznamu informácií poskytovaných dotknutej osobe, ak sú osobné údaje získané priamo od nej (čl. 13 GDPR, § 19 nového zákona o ochrane osobných údajov) a keď sú osobné údaje získané z iného zdroja (čl. 14 GDPR, § 20 nového zákona o ochrane osobných údajov)

poskytované informácie, ak sú osobné údaje získané priamo od dotknutej osoby	poskytované informácie, ak osobné údaje nie sú získané priamo od dotknutej osoby
identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	identifikačné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;
kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;	kontaktné údaje prevádzkovateľa a zástupcu prevádzkovateľa, ak bol poverený;
kontaktné údaje zodpovednej osoby, ak je určená;	kontaktné údaje zodpovednej osoby, ak je určená;
účel spracúvania osobných údajov, na ktorý sú osobné údaje určené;	účel spracúvania osobných údajov, na ktorý sú osobné údaje určené;
právny základ spracúvania osobných údajov;	právny základ spracúvania osobných údajov;
XXX	kategórie spracúvaných osobných údajov;
oprávnené záujmy prevádzkovateľa, ak sa osobné údaje spracúvajú na tomto právnom základe;	oprávnené záujmy prevádzkovateľa, ak sa osobné údaje spracúvajú na tomto právnom základe;
identifikácia príjemcu alebo kategória príjemcu, ak existuje;	identifikácia príjemcu alebo kategória príjemcu, ak existuje;
zamýšľaný prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, vrátane identifikácie tretej krajiny alebo medzinárodnej organizácie a identifikácie tzv. primeraných záruk;	zamýšľaný prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, vrátane identifikácie tretej krajiny alebo medzinárodnej organizácie a identifikácie tzv. primeraných záruk;
ďalšie doplňujúce informácie pre dotknutú osobu:	ďalšie doplňujúce informácie pre dotknutú osobu:
dobu uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia;	dobu uchovávania osobných údajov; ak to nie je možné, informácie o kritériách jej určenia;
o práve požadovať od prevádzkovateľa prístup k jej osobným údajom;	o práve požadovať od prevádzkovateľa prístup k jej osobným údajom;
o práve na opravu jej osobných údajov;	o práve na opravu jej osobných údajov;

o práve na vymazanie jej osobných údajov alebo o práve na obmedzenie spracúvania jej osobných údajov;	o práve na vymazanie jej osobných údajov alebo o práve na obmedzenie spracúvania jej osobných údajov;
o práve namietať spracúvanie osobných údajov;	o práve namietať spracúvanie osobných údajov;
o práve na prenosnosť osobných údajov;	o práve na prenosnosť osobných údajov;
o práve kedykoľvek svoj súhlas odvolať;	o práve kedykoľvek svoj súhlas odvolať;
o práve podať návrh na začatie konania na Úrad;	o práve podať návrh na začatie konania na Úrad;
XXX	o zdroji, z ktorého pochádzajú osobné údaje, prípadne informácie o tom, či pochádzajú z verejne prístupných zdrojov;
O tom, či je poskytovanie osobných údajov zákonnou požiadavkou, alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy a o tom, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj o možných následkoch neposkytnutia osobných údajov;	XXX
o existencii automatizovaného individuálneho rozhodovania, vrátane profilovania; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.	O existencii automatizovaného individuálneho rozhodovania, vrátane profilovania; v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takéhoto spracúvania osobných údajov pre dotknutú osobu.

Ako je vidieť z porovnania údajov v tabuľke, prevádzkovateľ musí informovať dotknutú osobu, ak ona sama nebola zdrojom poskytnutých osobných údajov, navyše aj o kategórii spracúvaných osobných údajov a o zdroji, z ktorého pochádzajú osobné údaje. Naopak, nie je povinný takejto dotknutej osobe poskytnúť informácie, či poskytnutie osobných údajov je zákonné/zmluvné/dobrovoľné/povinné, ani ju informovať o možných následkoch neposkytnutia osobných údajov. Kým informačná povinnosť prevádzkovateľa má byť plnená vo vzťahu k dotknutej osobe pri získavaní osobných údajov od nej samej, pri spracúvaní osobných údajov získaných z iného zdroja má prevádzkovateľ informačnú povinnosť plniť:

- najneskôr do jedného mesiaca po získaní osobných údajov, pričom zohľadní konkrétne okolnosti, za ktorých sa osobné údaje spracúvajú,
- najneskôr v čase prvej komunikácie s touto dotknutou osobou, ak sa osobné údaje majú použiť na komunikáciu s dotknutou osobou, alebo
- najneskôr vtedy, keď sa osobné údaje prvýkrát poskytnú, ak sa predpokladá poskytnutie osobných údajov ďalšiemu príjemcovi.

Aj keď nová právna úprava rozširuje plnenie informačnej povinnosti prevádzkovateľa aj na také spracúvanie, ktoré sa realizuje na právnom základe osobitného predpisu, na druhej strane rozširuje v porovnaní so starou právnou úpravou situácie, kedy **nemu**sí byť informačná povinnosť plnená v tých prípadoch, keď sa osobné údaje nezískavajú priamo od dotknutej osoby.

Tabuľka č. 4 Situácie, kedy nie je potrebné plniť informačnú povinnosť voči dotknutej osobe, ak osobné údaje neboli získané priamo od nej. Porovnanie starej a novej právnej úpravy.

Prevádzkovateľ nie je povinný informovať dotknutú osobu:

<i>podľa starej právnej úpravy</i>	<i>podľa novej právnej úpravy</i>
ak vie Úradu kedykoľvek na jeho žiadosť preukázať, že dotknutej osobe boli informácie už predtým poskytnuté;	v rozsahu, v akom dotknutá osoba už dané informácie má;
ak spracúva osobné údaje na právnom základe právneho predpisu (podľa § 10 ods. 1 a 2);	v rozsahu, v akom sa získanie týchto informácií alebo poskytnutie týchto informácií ustanovuje v osobitnom predpise, ktorý sa na prevádzkovateľa vzťahuje a v ktorom sú ustanovené primerané opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby (potreba prijatia opatrení zo strany prevádzkovateľa);
ak spracúva osobné údaje na účel tvorby umeleckých alebo literárnych diel, pre potreby informovania verejnosti masovokomunikačnými prostriedkami (podľa § 10 ods. 3 písm. a);	XXX
spracúva osobné údaje na historický výskum, alebo vedecký výskum a vývoj, alebo na účely štatistiky a poskytnutie takýchto informácií je objektívne nemožné, alebo by bolo možné len s vyvinutím neprimeraného úsilia;	v rozsahu, v akom sa poskytovanie týchto informácií ukáže ako nemožné, alebo by si vyžadovalo neprimerané úsilie, najmä ak sa spracúvajú osobné údaje na tzv. privilegované účely;
spracúva osobné údaje, ktoré už boli zverejnené v súlade so zákonom a prevádzkovateľ ich náležite označil ako zverejnené;	XXX
XXX	ak osobné údaje musia zostať dôverné na základe povinnosti mlčanlivosti podľa osobitného predpisu (zachovávanie profesijného tajomstva).

3.3.2 Právo na prístup

V porovnaní s právnou úpravou podľa starého zákona o ochrane osobných údajov nejde o nové právo priznané dotknutým osobám. Spresňuje sa však obsah, podmienky, obmedzenia a lehoty pre výkon tohto práva tak, aby každý občan Európskej únie mal rovnaké právo na prístup k svojim osobným údajom.

V súlade s článkom 15 GDPR a ust. § 21 nového zákona o ochrane osobných údajov právo na prístup zahŕňa tri čiastkové práva dotknutej osoby: *i)* právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má dotknutá osoba *ii)* právo získať prístup k týmto osobným údajom a *iii)* ďalšie informácie vymedzené v písm. a) až h) čl. 15 GDPR, resp. ust. § 21 ods. 1 nového zákona o ochrane osobných údajov.

i) právo získať potvrdenie

Prevádzkovateľ je povinný reagovať a odpovedať na každú žiadosť s otázkou: „*Spracúvate o mne osobné údaje?*“. Žiadosť nie je možné odignorovať a nereagovať s odôvodnením, že žiadosť nepodala dotknutá osoba vzhľadom na to, že prevádzkovateľ nespracúva žiadne osobné údaje žiadateľa. Máme za to, že odpovedať je potrebné aj v špecifických prípadoch, keď bude právo na prístup dotknutej osoby z niektorého zákonného dôvodu obmedzené. V takýchto prípadoch sa naformuluje neutrálna odpoveď „*nemôžeme ani potvrdiť, ani poprieť, že spracúvame vaše osobné údaje.*“ Súčasne však v odpovedi odporúčame informovať žiadateľa, že tým nie je nijako dotknuté jeho procesné právo na iniciovanie konania na Úrade, ktorý vykoná overenie zákonnosti obmedzenia práva na prístup i preskúma osobné údaje, ktorými prevádzkovateľ disponuje.

ii) právo získať prístup k osobným údajom

Prevádzkovateľ je povinný poskytnúť dotknutej osobe osobné údaje, ktoré spracúva. Prvá a jedna kópia výpisu, či odpisu spracúvaných osobných údajov sa poskytuje zdarma. Za ďalšie kópie dokumentov s osobnými údajmi, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, a ak nepožiadala o iný spôsob, prevádzkovateľ osobné údaje poskytne v bežne používanej elektronickej podobe. Dôvodom oprávňujúcim zamestnávateľa odmietnuť prístup dotknutej osoby k osobným údajom, sú nepriaznivé dôsledky na práva a slobody iných fyzických osôb.

Toto právo netreba vykladať tak, že zamestnávateľ je povinný sprístupniť zamestnancovi všetky svoje informačné systémy a fyzicky mu umožniť vstup do týchto systémov. To by bolo nakoniec aj v rozpore s bezpečnostnými štandardami ochrany osobných údajov. Garantuje sa právo na prístup k osobným údajom, nie právo na prístup k informačným systémom, ktoré sú usporiadanými súbormi osobných údajov. Rovnako tak nejde o právo zamestnanca na poskytnutie samotných dokumentov, na základe ktorých dochádza k spracúvaniu osobných údajov. Je vecou zamestnávateľa, v akej štrukturali-

zovanej forme poskytne osobné údaje, tak aby získaná informácia bola pre zamestnanca transparentná a zrozumiteľná.

iii) právo na ďalšie informácie

Je rozumné očakávať, že žiadosť sa spravidla neobmedzí len na jednoduchý záujem, či prevádzkovateľ spracúva osobné údaje. Dotknutá osoba si zvyčajne vyžiada ďalšie informácie a v tejto súvislosti má právo vedieť: na aký účel prevádzkovateľ spracúva jej osobné údaje; ktoré osobné údaje spracúva; komu prevádzkovateľ spracúvané osobné údaje poskytuje; ako dlho budú osobné údaje uchovávané; odkiaľ jej osobné údaje získal (informácie o zdroji, ak osobné údaje neposkytla sama dotknutá osoba) a aké primerané záruky ochrany osobných údajov prijal prevádzkovateľ pri prenose osobných údajov do tretej krajiny alebo medzinárodnej organizácii.

S uplatňovaním práva na prístup zo strany zamestnancov, ale aj bývalých zamestnancov, neúspešných uchádzačov o zamestnanie, rodinných príslušníkov či blízkych osôb zamestnancov musia zamestnávateľa počítať. Právo na prístup má pomerne široký rozsah a napríklad v rámci práva získať osobné údaje (viď bod *ii*)) sa zamestnanec od zamestnávateľa môže okrem klasického výpisu/odpisu zo svojho osobného spisu, domáhať záznamov z firemnej kroniky, poskytnutia kópie fotografie z teambuildingu a pod. Ak zamestnávateľ spracúva v súvislosti s dotknutou osobou veľké množstvo osobných údajov, môže požadovať, aby pred tým, ako dotknutej osobe poskytne požadované informácie, dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa jej žiadosť týka. Uplatnenie práva dotknutou osobou sa však nemôže stať podnetom, ani dôvodom na konanie zo strany zamestnávateľa, ktoré by dotknutej fyzickej osobe mohlo spôsobiť ujmu.

3.3.3 Právo na opravu

Podľa čl. 16 GDPR a ust. § 22 nového zákona o ochrane osobných údajov právo na opravu zahŕňa: **i) právo na to**, aby prevádzkovateľ bez zbytočného odkladu **opravil** nesprávne osobné údaje, ktoré sa týkajú dotknutej osoby a **ii) právo na doplnenie** neúplných osobných údajov so zreteľom na účel spracúvania osobných údajov. Uvedené je v korelácii so zásadou správnosti (čl. 5 písm. d) GDPR a § 9 nového zákona o ochrane osobných údajov), v zmysle ktorej spracúvané osobné údaje musia byť správne a podľa potreby aktualizované, aby nespôsobili dotknutej osobe žiadnu ujmu. Vedenie dotknutej osoby v zozname dlžníkov, aj potom, čo už dlh uhradila, je spôsobilé narušiť uplatňovanie jej ďalších práv a oprávnených záujmov súvisiacich s jej vnímaním ako insolventnej či finančne nedisciplinovanej.

Na chybu v spracúvaní osobných údajov môže prísť dotknutá osoba i prevádzkovateľ. Ak dotknutá osoba zistí, že osobné údaje, ktoré o nej prevádzkovateľ spracúva, sú nesprávne, má ho o tom upovedomiť a požiadať, aby ich opravil a nesprávne osobné údaje zlikvidoval. Ak zrejmu nesprávnosť zistí prevádzkovateľ z vlastnej činnosti, o zistení má dotknutú osobu informovať a požiadať ju, aby mu poskytla správne osobné úda-

je. Indikátorom, že zamestnávateľ spracúva nesprávne alebo neaktuálne osobné údaje môže byť napríklad vrátenie poštovej zásielky adresovanej zamestnancovi s informáciou „adresát neznámy“.

Je pritom úlohou prevádzkovateľa, aj bez žiadosti dotknutej osoby, prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili. Prevádzkovateľ nenesie zodpovednosť za spracúvanie nesprávnych osobných údajov, ak také poskytla sama dotknutá osoba, pokiaľ mu z osobitného predpisu nevyplyva povinnosť správnosť údajov preveriť.

Zodpovednosť za správnosť a aktuálnosť spracúvaných osobných údajov vo svojich informačných systémoch môžu zamestnávatelia zabezpečiť napríklad nastavením kontroly spracúvaných osobných údajov na nejakej pravidelnej báze. Nie je to však ich povinnosť, ale len odporúčanie. Rovnako zamestnávateľ nemá povinnosť žiadať každoročne od zamestnanca aktualizáciu jeho osobných údajov, aj keď tak robí napríklad vo vzťahu aktualizácii zdravotnej poisťovne. V súlade so zákonom č. 580/2004 Z. z. o zdravotnom poistení v znení neskorších predpisov má každý poistenec právo na zmenu zdravotného poistenia.⁵⁵ Ak je poistenec zamestnancom, **je povinný** zmenu príslušnej zdravotnej poisťovne oznámiť zamestnávateľovi a to do ôsmich dní odo dňa každej zmeny príslušnej zdravotnej poisťovne (t. j. do 9. januára 2018, ak poistenec podal prihlášku do 30. septembra 2017). Ak je zamestnancom u viacerých zamestnávateľov, je povinný uvedené skutočnosti oznámiť každému zamestnávateľovi (§ 23 ods. 6 zákona o zdravotnom poistení). Pri nesplnení tejto oznamovacej povinnosti hrozí poistencovi pokuta od Úradu pre dohľad nad zdravotnou starostlivosťou SR až do výšky 331 eur (§ 26 ods. 1 písm. b) zákona o zdravotnom poistení). Splnenie tejto povinnosti zamestnancom je pre zamestnávateľa, ako platiteľa poistného na zdravotné poistenie, dôležité. Z pôvodnej zdravotnej poisťovne, z ktorej zamestnanec odišiel, je zamestnávateľ povinný zamestnanca odhlásiť a prihlásiť ho do novej zdravotnej poisťovne, ktorú si zamestnanec vybral, a preto zamestnávatelia často dobrovoľne vyzývajú svojich zamestnancov na aktualizáciu toho údaj, aj keď nemusia.

3.3.4 Právo na vymazanie (právo „na zabudnutie“)

Právo na výmaz predstavuje inými slovami vyjadrenú povinnosť prevádzkovateľa zlikvidovať osobné údaje. V súlade s čl. 17 GDPR a ust. § 23 nového zákona o ochrane osobných údajov má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú, a to v týchto prípadoch:

- a) osobné údaje už nie sú potrebné na účel, na ktorý prevádzkovateľ tieto údaje získal, alebo spracúval;
- b) dotknutá osoba odvolá svoj súhlas, a neexistuje iný právny základ pre spracúvanie osobných údajov;

⁵⁵ Bližšie k tomu: ŽULOVÁ, J. Chcete zmeniť zdravotnú poisťovňu? In: Práca a Mzdy bez chýb, pokiaľ a penále. - ISSN 1337-060X. - Roč. XI. č. 7-8 (2016), s. 3-4.

- c) dotknutá osoba namieta spracúvanie osobných údajov (viď kapitola 3.3.7.) a ne-
prevažujú žiadne oprávnené dôvody na spracúvanie osobných údajov;
- d) osobné údaje sa spracúvajú nezákonne;
- e) dôvodom pre výmaz je splnenie povinnosti podľa zákona o ochrane osobných
údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská
republika viazaná;
- f) osobné údaje sa získavali v súvislosti s ponukou služieb informačnej spoločnosti
podľa čl. 8 ods. 1 GDPR alebo § 15 ods. 1 nového zákona o ochrane osobných
údajov.

Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracúvaním osobných údajov, ktoré sa jej týkajú, pričom súhlas môže odvolať rovnakým spôsobom, akým súhlas udelila. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založenom na súhlase pred jeho odvolaním. Odvolanie súhlasu nemusí vždy pre prevádzkovateľa predstavovať aj povinnosť zlikvidovať osobné údaje, keďže súhlas bol daný k určitým účelom. Po odvolaní súhlasu je prevádzkovateľ povinný prestať spracúvať osobné údaje „len“ pre ten účel, ku ktorému bol súhlas udelený a následne odvolaný. Rovnako v prípade, že prevádzkovateľ použil súhlas pre prípady, keď spracúvaniu osobných údajov svedčí iný právny dôvod (predovšetkým ide o spracúvanie na základe zákona), neznamená odvolanie súhlasu (teda úkonu, ktorý nebol nevyhnutný pre spracúvanie) povinnosť prevádzkovateľa prestať spracúvať, či zlikvidovať spracúvané osobné údaje.

Povinnosťou prevádzkovateľa, ak spracúval osobné údaje na základe súhlasu dotknutej osoby, ktorý potom pred uplynutím času jeho platnosti odvolala, bolo podľa starej právnej úpravy blokovat' jej osobné údaje. Blokovanie osobných údajov sa podľa ust. § 23 ods. 3 písm. a) bod 6 starého zákona o ochrane osobných údajov rozumelo *dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého bolo možné vykonávať len tie operácie s osobnými údajmi, ktoré boli nevyhnutné na splnenie povinnosti uloženej zákonom o ochrane osobných údajov*. Nový zákon o ochrane osobných údajov výslovne spracovateľskú operáciu, akou je blokovanie, neupravuje (ekvivalentom je obmedzenie spracúvania, bližšie kapitola 3.3.5) a povinnosťou prevádzkovateľa je po odvolaní súhlasu osobné údaje vymazať, pokiaľ sa neuplatňuje niektorá z výnimiek oslobodzujúca ho od tejto povinnosti. Blokovanie osobných údajov bolo možné vnímať ako určitý medzistupeň, keď osobné údaje ešte nebolo vhodné rovno zlikvidovať, ale zas bolo nutné pozastaviť ich ďalšie spracúvanie. Napríklad, ak zamestnávateľ evidoval osobné údaje zamestnanca na základe jeho súhlasu v rozsahu titul, meno, priezvisko, adresa a pracovné hodnotenie na účel poskytnutia benefitu vo forme zamestnaneckej zľavy na nákup tovaru a poskytnutie služieb, ktoré štandardne predáva/poskytuje svojim klientom a zamestnanec sa rozhodol odvolať svoj súhlas so spracúvaním osobných údajov na účel poskytovania takéhoto benefitu, zamestnávateľ namiesto likvidácie pristúpil k blokovaniu. Ak by z poskytnutého benefitu plynuli práva alebo povinnosti na

strane zamestnávateľa alebo zamestnanca, blokovanie osobných údajov mohol zamestnávateľ uchovávať do doby pominutia právnych nárokov.

V prípade, že prevádzkovateľ zverejnil osobné údaje dotknutej osoby a tá žiada osobné údaje vymazať, uplatňovanie práva na výmaz sa **rozširuje o právo na zabudnutie**. Prevádzkovateľ, zohľadniac svoje technologické možnosti, prostriedky a náklady na vykonanie, je povinný informovať ďalších prevádzkovateľov, ktorým poskytol osobné údaje dotknutej osoby, že táto žiada o výmaz jej osobných údajov.⁵⁶ „Vynovené“ právo na výmaz tak zhrňa nielen právo na vymazanie osobných údajov, ale aj zdržanie sa ďalšieho šírenia týchto údajov a povinnosť prevádzkovateľov údajov, ktorí sprístupnili údaje, aby informovali tretie strany o žiadosti dotknutého subjektu o vymazanie všetkých kópií i odkazov na tieto osobné údaje.

Prevádzkovateľ **nie je povinný** osobné údaje dotknutej osoby **vymazať** a tá musí ich spracúvanie strpieť, ak existuje niektorý z nasledujúcich taxatívnych zákonných dôvodov:

- a) v danej situácii ide o uplatnenie práv na slobodu prejavu alebo práva na informácie;
- b) ide o splnenie povinnosti podľa zákona o ochrane osobných údajov, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme, alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- c) z dôvodov verejného záujmu v oblasti verejného zdravia;
- d) na účel archivácie, na vedecký účel, na účel historického výskumu, alebo na štatistický účel, ak je pravdepodobné, že právo na výmaz znemožní alebo závažným spôsobom sťaží dosiahnutie cieľov takého spracúvania;
- e) na uplatnenie právneho nároku.

3.3.5 Právo na obmedzenie spracúvania

Právo dotknutej osoby na obmedzenie spracúvania znamená, že prevádzkovateľ pozastavuje ďalšie spracovateľské operácie s osobnými údajmi, t. j. osobné údaje „len“ uchováva a ďalej nepoužíva. Spracovávané osobné údaje, vo vzťahu ku ktorým sa uplatňuje právo na obmedzenie spracúvania, sa označia s cieľom obmedziť ich spracúvanie v budúcnosti. Dotknutá osoba má právo žiadať od prevádzkovateľa, aby obmedzil spracúvanie jej osobných údajov:

- a) na čas, kým prevádzkovateľ overuje správnosť osobných údajov, ak dotknutá osoba namieta správnosť spracúvaných osobných údajov;
- b) namiesto vymazania, ak je spracúvanie osobných údajov nezákonné;

⁵⁶ Explicitné vyjadrenie práva na výmaz, resp. práva na zabudnutie je reakciou na rozsudok Súdneho dvora EÚ z 13. mája 2014 C-131/12 Google Spain SL vs. Mario Costeja González, ktorý uznal ako odôvodnené právo španielskeho občana na vymazanie jeho osobných údajov internetovým vyhľadávačom – spoločnosťou Google tak, aby jeho osobné údaje nemohli byť pri vyhľadávaní jeho osobou viditeľné.

- c) na čas, keď ich dotknutá osoba potrebuje na uplatnenie právneho nároku, aj keď prevádzkovateľ už nepotrebuje osobné údaje na účel, na ktorý sa osobné údaje spracúvali;
- d) na čas, kým sa overuje, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby, ak sa osobné údaje spracúvajú na tomto právnom základe.

Ak je spracúvanie osobných údajov dotknutej osoby na základe jej žiadosti obmedzené, môže prevádzkovateľ ďalšie spracovateľské operácie s takýmito údajmi realizovať len na základe súhlasu dotknutej osoby. Súhlas nepotrebuje na spracovateľské operácie ako uchovávanie, preukazovanie a obhajovanie právnych nárokov, na ochranu fyzickej osoby alebo právnickej osoby, alebo z dôvodov verejného záujmu.

Pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené, je prevádzkovateľ povinný o tejto skutočnosti informovať dotknutú osobu.

3.3.6 Právo na prenosnosť osobných údajov

Právo na prenosnosť (čl. 20 GDPR a ust. 26 nového zákona o ochrane osobných údajov) je novým právom priznaným dotknutej osobe, ktoré má posilniť jej kontrolu nad vlastnými osobnými údajmi a umožniť jej získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte. Aj keď úzko súvisí s právom na prístup, odlišuje sa od neho. Cieľom práva na prenosnosť osobných údajov je uľahčiť dotknutým osobám premiestňovanie, kopírovanie či preskupovanie vlastných osobných údajov z jedného informačného prostredia do druhého (či už do vlastných systémov, systémov dôveryhodných tretích strán, alebo systémov nových prevádzkovateľov).

Právo na prenosnosť zahŕňa údaje, ktoré sa dotknutej osoby týkajú a ktoré poskytla prevádzkovateľovi, vrátane pseudonymizovaných údajov, nie však údajov anonymných alebo anonymizovaných (vysvetlené v kapitole 2.2.1.). Pracovná skupina WP 29 vysvetľuje, že osobné údaje, ktoré dotknutá osoba poskytla prevádzkovateľovi, zahŕňajú dve kategórie údajov:

- a) údaje aktívne a vedome poskytnuté dotknutou osobou (napríklad poštová adresa, užívateľské meno, vek ...);
- b) vypozerované údaje poskytnuté dotknutou osobu na základe požívania služby alebo zariadenia (napr. história vyhľadávania, údaje o prevádzke a lokalizačné údaje osoby, pulz sledovaný nositeľným zariadením a pod.).⁵⁷

Vypozerované údaje ale nezahŕňajú údaje vytvorené prevádzkovateľom, aj keď tie boli vytvorené zo vstupných, vedome poskytnutých, alebo vypozerovaných údajov. Ak

⁵⁷ Výkladové usmernenie WP č. 242 rev. 01 k právu na prenosnosť osobných údajov z 13. decembra 2016 a revidované v apríli 2017. Dostupné na: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm (ďalej len stanovisko WP č. 242 rev. 01).

zamestnávateľ vytvorí „zdravotný profil“ uchádzača o zamestnanie, či zamestnanca na základe analýzy údajov zhromaždených z lekárskeho prehliadok vo vzťahu k práci, nepôjde o kategóriu osobných údajov, ktoré by bolo možné subsumovať pod prenositeľné osobné údaje. Výsledok posúdenia, týkajúci sa zdravotného stavu zamestnanca, nemôže byť sám osebe považovaný za údaj poskytnutý dotknutou osobou. Je úlohou prevádzkovateľa posúdiť a možno aj vopred vhodne zadefinovať, ktoré osobné údaje v jeho vlastných systémoch patria do pôsobnosti práva na prenositeľnosť.

V konkrétnych aspektoch právo na prenosnosť osobných údajov znamená právo dotknutej osoby:

i. *získať tie údaje, ktoré sa jej týkajú a ktoré prevádzkovateľovi poskytl;*

Nie je podmienkou, že dotknutá osoba bude svoje osobné údaje ďalej prenášať, môže ich sama spracúvať na vlastné súkromné účely. Realizácia tohto práva ponúka dotknutej osobe uľahčenie spôsobu ako spravovať a opätovne používať svoje osobné údaje. Pri aplikácii na pracovnoprávne vzťahy si vieme predstaviť žiadosť zamestnanca o poskytnutie zoznamu nákupov, ktoré zrealizoval na základe poskytnutej zamestnaneckej (vernostnej) karty.

ii. *preniesť osobné údaje bez obmedzení k ďalšiemu prevádzkovateľovi bez toho, aby jej v tom pôvodný prevádzkovateľ nejakým spôsobom bránil;*

Prevádzkovateľ nesmie vytvárať žiadne (právne, technické, finančné) prekážky, ktoré by bránili v prenositeľnosti údajov. Údaje má poskytnúť v interoperabilnom formáte, ale na druhej strane nie je povinný zavádzať technicky kompatibilné systémy s ďalšími prevádzkovateľmi. Ako vhodný formát ale nie je posúdený taký formát, ktorého používanie podlieha nákladnému zakúpeniu licencie, ani formát, ktorý neumožní opätovné použitie osobných údajov.⁵⁸ Prevádzkovateľ by mal pri voľbe formátu vždy vziať do úvahy, ako tento formát ovplyvní právo dotknutej osoby opätovne použiť jej údaje. Prenositeľnosť osobných údajov má uľahčiť opätovné použitie osobných údajov medzi užívateľmi rôznych služieb, o ktoré majú záujem.

iii. *požadovať od prevádzkovateľa, aby on preniesol jej osobné údaje k druhému prevádzkovateľovi, ak je to technicky možné;*⁵⁹

Vzhľadom na to, že prevádzkovateľ nevyberá príjemcu, ku ktorému sa prenášajú osobné údaje dotknutej osoby, nemôže ani zodpovedať za to, či prijímajúca strana dodržiava zásady ochrany osobných údajov. „Príjemca“ prenesených osobných údajov sa stáva novým prevádzkovateľom so všetkými prislúchajúcimi povinnosťami. Jeho prvý krok by mal smerovať k určeniu účelu spracúvania prenesených osobných údajov a pl-

58 Ako príklad nevhodného formátu sa uvádza poskytnutie PDF verzie emailov. Podľa stanoviska WP č. 242 rev. 01 PDF verzia emailov nie je dostatočne štruktúrovaná a natoľko deskriptívna, aby sa dotknutej osobe umožnilo ľahké opätovné použitie osobných údajov z takejto pošty.

59 Výkladové stanovisko WP č. 242 rev. 01 odporúča využiť dva nástroje pre odpovede na žiadosti dotknutých subjektov na prenosnosť ich osobných údajov: po prvé dotknutej osobe by mali ponúknuť možnosť priameho stiahnutia spracúvaných osobných údajov a po druhé by jej mali umožniť priamy prenos jej osobných údajov k ďalšiemu subjektu, napríklad prostredníctvom poskytnutia rozhrania pri programovaní aplikácií, tzv. Application Programming Interface.

neniu informačnej povinnosti (viď kapitola 3.3.1. Právo na informácie). Subjekt, ku ktorému sú prenášané osobné údaje dotknutej osoby, má právo prijať, ale aj odmietnuť prenášané osobné údaje.

iv. naďalej pokračovať vo využívaní „služieb“ prevádzkovateľa.

Prenositelnosť osobných údajov automaticky nevedie k výmazu prenesených osobných údajov u pôvodného prevádzkovateľa a nijako ani neovplyvňuje dobu uchovávania spracúvaných osobných údajov.

Právo na prenosnosť osobných údajov nepatrí dotknutej osobe v neobmedzenom rozsahu. Vzťahuje sa na presne vymedzené spracovateľské operácie. Právo žiadať o prenosnosť osobných údajov má dotknutá osoba za predpokladu, že spracúvanie osobných údajov sa u prevádzkovateľa vykonáva **automatizovanými prostriedkami** a na niektorom z týchto dvoch uvedených právnych základoch:

- i. na základe súhlasu (podľa čl. 6 ods. 1 písm. a) alebo čl. 9 ods. 2 písm. a) GDPR, resp. § 13 ods. 1 písm. a) a § 16 ods. 2 písm. a) nového zákona o ochrane osobných údajov), alebo
- ii. spracúvanie založené na zmluvnom vzťahu (t. j. spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby podľa čl. článku 6 ods. 1 písm. b) GDPR, resp. § 13 ods. 1 písm. b) nového zákona o ochrane osobných údajov).

Je potrebné si tiež uvedomiť, že právo na prenositeľnosť osobných údajov neukladá prevádzkovateľovi povinnosť uchovávať osobné údaje dlhšiu dobu, než je nevyhnutné, resp. stanovené právnym predpisom. Právo na prenositeľnosť dotknutých osobných údajov tak nebude zo strany dotknutej osoby využiteľné, ak použiteľná doba uchovávania osobných údajov už uplynula a prevádzkovateľ už osobné údaje nemá.

Právo na prenositeľnosť osobných údajov sa neuplatní, ak je spracúvanie založené na inom právnom základe, než je súhlas alebo spracúvanie na účely zmluvy, čo znamená, že toto právo sa nebude uplatňovať vo vzťahu ku akýmkoľvek osobným údajom, ktoré prevádzkovateľ spracúva, ale len na tie osobné údaje, na ktorých spracúvanie poskytla dotknutá osoba súhlas alebo na tie, ktorých spracúvanie je potrebné na plnenie zmluvy. Napríklad, ak zamestnanec používa zamestnaneckú e-mailovú adresu a pri odchode zo zamestnania by požiadal zamestnávateľa o prenos svojich emailových kontaktov (adresára),⁶⁰ zamestnávateľ mu nie je podľa nášho názoru povinný vyhovieť, pretože spracúvanie takýchto údajov nebolo založené ani na súhlase dotknutej osoby, ani na zmluve, v ktorej je zamestnanec zmluvnou stranou.

Z uvedeného nám vyplýva, že v pracovnoprávných vzťahoch bude uplatniteľnosť práva na prenosnosť osobných údajov zo strany zamestnancov pomerne nízka. Vzhľa-

⁶⁰ Samostatnou otázkou je, či sú profesionálne alebo aj neprofesionálne kontakty zamestnanca obsiahnuté v adresári zamestnaneckého e-mailového účtu jeho osobnými údajmi, alebo ide o „vlastníctvo“ zamestnávateľa.

dom na nerovnováhu medzi zamestnávateľom a zamestnancom sa z povahy veci v mnohých prípadoch nebude súhlas zamestnanca považovať za slobodný (bližšie kapitola 2.3.2.). Väčšina osobných údajov zamestnancov v ich personálnych spisoch sa spracúva na právnom základe podľa čl. 6 ods. 1 písm. c) alebo § 13 ods. 1 písm. c) nového zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. V prípade osobných údajov zamestnancov sa tak právo na prenosnosť spravidla použije iba vtedy, ak je spracúvanie založené na zmluve, ktorou je zamestnanec stranou. Uplatniteľnosť práva na prenositeľnosť osobných údajov v pracovnoprávných vzťahoch prichádza teda do úvahy pri prenose tých osobných údajov, ktoré sú identifikačnými údajmi zmluvnej strany pri uzatváraní pracovnej zmluvy alebo niektorej z dohôd o prácach vykonávaných mimo pracovného pomeru, resp. tých osobných údajov, ktoré sú na plnenie pracovnej zmluvy alebo niektorej z dohôd o prácach vykonávaných mimo pracovného pomeru nevyhnutné. Podmienkou je však to, že tieto identifikačné údaje, alebo údaje potrebné na plnenie pracovnej zmluvy, či dohody, sú spracúvané automatizovanými prostriedkami. Ak zamestnávateľ vedie pracovné zmluvy, či dohody v listinnej podobe (čo je bežnou praxou), právo na prenositeľnosť údajov sa nepoužije, pretože spracúvanie osobných údajov nie je uskutočňované automatizovane.

3.3.7 Právo namietat'

Právo namietat' spracúvanie osobných údajov patrí dotknutej osobe vtedy, ak sa domnieva, že spracúvanie už obmedzuje jej práva, alebo do nich zasahuje a ak sa spracúvanie uskutočňuje:

- i. na právnom základe podľa čl. 6 ods. 1 písm. e) GDPR alebo ust. § 13 ods. 1 písm. e) nového zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;
- ii. na právnom základe podľa čl. 6 ods. 1 písm. f) GDPR alebo ust. § 13 ods. 1 písm. f) nového zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany; alebo
- iii. na účel priameho marketingu, vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom.

Dôsledkom namietania spracúvania je to, že prevádzkovateľ ďalej nesmie spracúvať osobné údaje dotknutej osoby, pokiaľ nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku. V prípade spracúvania osobných údajov na účely priameho marketingu výnimka neexistuje, a namietanie spracúvania na tieto účely má vždy za následok zastavenie ďalšieho spracúvania osobných údajov.

Dotknutá osoba nemá právo namietiť spracúvanie osobných údajov, ak ide o spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu a spracúvanie na vedecký účel, na účel historického výskumu alebo na štatistický účel, t. j. na tzv. privilegované účely.

3.3.8 Právo na neúčinnosť automatizovaného individuálneho rozhodovania, vrátane profilovania

Automatizované systémy už nie sú len súčasťou výroby, ale prenikajú aj do rozhodovania. Počítačové algoritmy dokážu spracúvať veľké množstvo rozmanitých vstupných parametrov, prepojiť ľudskými schopnosťami nepostrehnuteľné väzby a vyprodukovať využiteľné výsledky vo veľmi krátkom čase. Dokážu si samé získať vstupné údaje z rôznych zdrojov (najmä v online prostredí), bez zaujatosti a emócií vyhodnotiť ľudské vlastnosti i schopnosti a predpovedať tak napríklad kvalitu uchádzača o zamestnanie.⁶¹

Profilovanie a automatizované spracúvanie sú modernými podpornými prostriedkami pri rozhodovaní v rastúcom počte oblastí. Nedokážu však vziať do úvahy okolnosti konkrétneho prípadu hodné osobitného zreteľa, a tak samotné profilovanie a následne i rozhodnutie prijaté na automatizovanom spracúvaní môže byť nesprávne i nespravodlivé. Preto čl. 22 GDPR a ust. § 28 nového zákona o ochrane osobných údajov priznávajú dotknutej osobe *právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov, vrátane profilovania a ktoré má právne účinky, ktoré sa jej týkajú, alebo ju obdobne významne ovplyvňujú.*

Profilovanie je podľa čl. 4 ods. 4 GDPR a podľa ust. § 5 písm. g) nového zákona o ochrane osobných údajov *akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúca v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom.* Profilovanie nie je *a priori* GDPR ani novým zákonom o ochrane osobných údajov zakázané. Je však dôležité, aby bolo profilovanie predvídateľné, a aby sa uskutočňovalo na základe zákonných pravidiel.

Automatizované rozhodovanie predstavuje možnosť rozhodovať čisto technologickými prostriedkami na základe ľubovoľného druhu údajov. Nie je podstatné, či je automatizované rozhodovanie výsledkom posúdenia údajov poskytnutých samotnými jednotlivcami, vypozerovaných, odvodených, či vyvedených dát. Podstatné je, že ide o rozhodnutie bez ľudského zásahu. Automatizované rozhodovanie môže byť usku- točnené s použitím profilovania alebo aj bez neho, profilovanie je možné realizovať

61 VOJTKO, Jakub. Automatizované rozhodovanie a profilovanie v pracovnoprávných vzťahoch podľa Všeobecného nariadenia o ochrane údajov. IN: Časopis pro právní vědu a praxi. [Online]. 2017, č. 2, s. 255-274. [cit. 2017-11-14]. Dostupné z: <https://journals.muni.cz/cpv/article/view/6322>.

aj bez automatizovaného rozhodovania.⁶² Prevádzkovateľ zadáva na začiatku vstupné parametre (spravidla osobné údaje dotknutej osoby v rôznom rozsahu), ktoré vytvorená aplikácia alebo určený algoritmus vyhodnotia a vygenerujú výsledok. Takto generované rozhodnutie môže mať na dotknutú osobu významný vplyv a môže založiť voči nej právne účinky. Ako sme už uviedli vyššie, vygenerovaná informácia o určitých vlastnostiach, či predispozíciách môže ovplyvniť zamestnávateľa, ktorý sa rozhodne výsledky využiť na zamietnutie žiadosti uchádzača o prijatie do pracovného pomeru. A aj keď vstupné zadávané parametre navonok pôsobia neutrálne, nie je možné s istotou vylúčiť, že vo vzájomných kombináciách ide v podstate o chránené charakteristiky, na ktoré by sa z dôvodu rešpektovania zásady rovnakého zaobchádzania vôbec nemalo prihliadať.

Rovnako ako v prípade profilovania GDPR, ani nový zákon o ochrane osobných údajov generálne nezakazujú rozhodovanie založené na profilovaní, ale v prípade použitia výlučne automatizovaného rozhodovania, vrátane profilovania,⁶³ priznávajú dotknutej osobe právo *na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú, alebo ju podobne významne ovplyvňujú* (čl. 22 ods. 1 GDPR a § 28 ods. 1 nového zákona o ochrane osobných údajov). Zákaz automatizovaného rozhodovania, vrátane profilovania, sa uplatní len za predpokladu, že:

i. rozhodnutie alebo profilovanie je založené výlučne na automatizovanom spracúvaní osobných údajov a

Je momentálne otáznе, čo presne sa bude rozumieť ľudskou intervenciou, ktorá znemožní dotknutej osobe uplatňovanie jej práva vylúčiť automatizované rozhodovanie. Sme toho názoru, že výber parametrov vstupujúcich do profilovania/automatizovaného spracúvania, ako aj formálne potvrdenie, či prijatie výsledkov takejto činnosti doze-rajúcou osobou sú ľudské zásahy neohrozujúce výlučnosť automatizovaného procesu. O výlučne automatizovanom spracúvaní môžeme hovoriť, ak konečné rozhodnutie nie je ovplyvnené žiadnym ďalším faktorom, ktorý by vzala do úvahy ľudská bytosť.

ii. rozhodnutie má právne účinky, ktoré sa dotknutej osoby týkajú, alebo ju podobne významne ovplyvňujú.

62 Ako príklad Stanovisko WP č. 251 k automatizovanému individuálnemu rozhodovaniu a profilovaniu z 3. októbra 2017 uvádza, že automatizovaným rozhodovaním nezahrňujúcim profilovanie je ukladanie pokút za rýchlosť len na základe dôkazu z kamier merajúcich rýchlosť. O automatizované rozhodovanie, vrátane profilovania by išlo vtedy, ak by nejaký čas bolo správanie jednotlivca na cestách pozorované a výška pokuty by bola potom odstupňovaná v závislosti od toho, koľkokrát a v akom období sa už jednotlivec dopustil priestupkov na úseku cestnej premávky.

63 Príkladom rozhodovania založeného na profilovaní je situácia, ak o pozvaní na pracovný pohovor rozhodne personalista, a to na základe profilu vytvoreného čisto za pomoci automatizovaných (technických) prostriedkov. Príkladom výhradne automatizovaného rozhodovania, vrátane profilovania je situácia, ak o pozvaní na pracovný pohovor rozhoduje algoritmus a pozvánka je doručená vhodným potenciálnym uchádzačom o zamestnanie bez akéhokoľvek ľudského zásahu.

Rozhodnutie má právne účinky vtedy, ak spôsobuje vznik, zmenu, zánik práv alebo povinností dotknutej osoby, resp. znemožňuje dotknutej osobe výkon jej práva. Ak teda zamestnávateľ využíva aplikácie na vyhodnotenie čo najvhodnejšieho kandidáta na obsadzované pracovné miesto, alebo vyhodnotenie pracovných výkonov zamestnancov s priznaním/nepriznaním variabilnej zložky mzdy, je jeho činnosť automatizovaným spracúvaním s právnymi účinkami a zamestnanec má právo žiadať, aby sa na neho takéto rozhodovanie nevzťahovalo.

Podľa článku 22 ods. 2 GDPR a ust. § 28 ods. 2 nového zákona o ochrane osobných údajov však dotknutá osoba nemá právo žiadať vylúčenie automatizovaného rozhodovania vo vzťahu k svojej osobe, ak je automatizované spracúvanie:

- a) *nevyhnutné pre uzavretie alebo na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom; alebo*

Zamestnávateľ môže mať záujem na využití automatizovaného rozhodovania z viacerých dôvodov. Automatizované rozhodovanie šetrí čas pri spracúvaní väčšieho množstva dát, zlepšuje účinnosť rozhodovacieho procesu, eliminuje chyby spôsobené ľudským faktorom. Je potrebné si však uvedomiť, že využitie automatizovaného rozhodovania podmieňuje nevyhnutnosť. Napríklad rozhodnutím potrebným na plnenie záväzkov z pracovnej zmluvy môže byť rozhodnutie zamestnávateľa o rozvrhovaní pracovného času.⁶⁴ Ak zamestnávateľ využíva na plánovanie a rozvrhovanie pracovných zmien zamestnancov počítačový program, ide o automatizované rozhodovanie. To, či zamestnanec môže voči svojej osobe vylúčiť takéto automatizované rozhodovanie záleží od toho, či takýto druh spracúvania je, alebo nie je **nevyhnutný** na plnenie pracovnej zmluvy. Nevyhnutnosť má byť pritom posudzovaná s prihliadnutím na to, či by na dosiahnutie rovnakého cieľa mohla byť zvolená aj iná, menej invazívna metóda. Prikláňame sa k názoru, že rozvrhovanie pracovných zmien, ktoré je výsledkom automatizovaného rozhodovania, nie je spôsobilé zasiahnuť do práv dotknutej osoby natoľko vážne, že by malo byť *a priori* vylúčené. Všetko však závisí od posúdenia okolností konkrétneho prípadu, pretože naprogramovaná aplikácia nie je automaticky zárukou, že sú rešpektované všetky zákonné aspekty rozvrhovania pracovného času.

- b) *vykonané na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, a v ktorých sú zároveň ustanovené aj vhodné opatrenia zaručujúce ochranu práv a oprávnených záujmov dotknutej osoby; alebo*

Podľa recitálu 71 GDPR by mohlo ísť o prípady automatizovaného spracúvania napríklad na účely monitorovania podvodov a daňových únikov a ich predchádzaniu, ktoré sa uskutočňuje v súlade s právnym predpismi, normami a odporúčaniami inštitúcií Európskej únie alebo vnútroštátnych orgánov dozoru a na zaistenie bezpečnosti a spoľahlivosti služby poskytovanej zo strany prevádzkovateľa.

⁶⁴ Záznamy o pracovnom čase sú osobnými údajmi zamestnanca. K tomu rozhodnutie Súdneho dvora EÚ C-342/12 vo veci Worten – Equipamentos para o Lar, SA proti Autoridade para as Condições de Trabalho (ACT) z 30. mája 2013.

- c) *založené na výslovnom súhlase dotknutej osoby s takouto formou jeho spracúvania.*⁶⁵

Súhlas nie je právne relevantným základom pre spracúvanie, ak dotknutá osoba nemá na výber, napríklad v situáciách, kde je súhlas s automatizovaným spracúvaním nevyhnutným predpokladom poskytnutia služby alebo v situáciách, kde je nerovnováha síl, ako napríklad vo vzťahu zamestnávateľ – zamestnanec. Prevádzkovateľ, ktorý sa spolieha na súhlas, ako na právny základ automatizovaného spracúvania, bude musieť preukázať, že dotknuté osoby presne chápu, k čomu súhlas udeľujú (pozri ďalej).

Je potrebné si uvedomiť, že tieto tri právne základy (a) až (c) sa vzťahujú na využívanie rozhodovania, ktoré je založené výlučne na automatizovanom spracúvaní. Vo vzťahu k profilovaniu sú využiteľné také právne základy ako pri spracúvaní všeobecných (bežných) a citlivých osobných údajov (viď kapitola 2.3.2. Zákonnosť spracúvania).

Dotknutá osoba v prípadoch a) a c) neostáva celkom bez ochrany. Síce nemôže žiadať úplne vylúčenie automatizovaného rozhodovania vo vzťahu k svojej osobe, no môže požiadať prevádzkovateľa o preverenie výsledku prostredníctvom neautomatizovaného zásahu (tzv. **právo na ľudský zásah**), má právo vyjadriť svoje stanovisko a tiež právo napadnúť rozhodnutie.

Dotknutá osoba je chránená aj v tom smere, že automatizované rozhodovanie, ktoré pracuje s citlivými osobnými údajmi, je dovolené len za určitých výnimiek. Menovite vtedy, ak sa uplatňuje spracúvanie citlivých osobných údajov na základe výslovného súhlasu dotknutej osoby (čl. 9 ods. 2 písm. a) GDPR a ust. § 16 ods. 2 písm. a) nového zákona o ochrane osobných údajov) alebo z dôvodu verejného záujmu (čl. 9 ods. 2 písm. g) GDPR a ust. 16 ods. 2 písm. g) nového zákona o ochrane osobných údajov) a súčasne sú zavedené vhodné opatrenia na zaručenie práv a oprávnených záujmov dotknutej osoby.

Pre účinné uplatňovanie vyššie uvedených práv dotknutej osoby právna úprava zdôrazňuje povinnosť prevádzkovateľa poskytnúť dotknutej osobe informácie o existencii automatizovaného individuálneho rozhodovania, vrátane profilovania. Konkrétne prevádzkovateľ poskytne dotknutej osobe zmysluplné informácie o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takehoto spracúvania (viď kapitola 3.3.1 Právo na informácie). Je úlohou prevádzkovateľa nájsť jednoduchý spôsob, ako dotknutej osobe vysvetliť podstatu a kritériá, na ktorých automatizované rozhodovanie spočíva. Nejde o to, aby dotknutej osobe vysvetlil, alebo odhalil celý algoritmus, poskytnutá informácia však má by pre dotknutú osobu zmysluplná. Právo na prístup oprávňuje dotknuté osoby na získanie rovnakých informácií o výlučnom automatizovanom rozhodovaní, vrátane profilovania (viď kapitola 3.3.2 Právo na prístup).

⁶⁵ K výslovnému súhlasu pozri kapitolu 2.3.2.2. Druhy právnych základov pri spracúvaní citlivých osobných údajov.

3.3.9. Povinnosti prevádzkovateľa (zamestnávateľa) pri uplatňovaní práv dotknutej osoby

Na predchádzanie akýmkoľvek nejasnostiam, na preukázanie splnenia povinností v súlade s čl. 12 GDPR a ust. § 29 nového zákona o ochrane osobných údajov a predovšetkým pre zjednodušené a transparentné uplatňovanie práv, možno odporučiť vypracovanie vnútropodnikovej dokumentácie k uplatňovaniu vyššie uvedených práv dotknutej osoby, v ktorej zamestnávateľ jasne a zrozumiteľne uvedie a zhrnie:

- I. **Kontaktné údaje** osoby poverenej vybavovaním žiadostí a poskytovaním informácií k uplatňovaniu práv dotknutej osoby (meno, priezvisko, doručovacia adresa, emailová adresa, fax, telefónne číslo). Úlohou môže byť poverená *tzv. zodpovedná osoba* (k vysvetleniu pozri ďalej).⁶⁶
- II. **Spôsob** a formu spätnej reakcie, napríklad, že odpovede na žiadosti k uplatňovaniu práv a informácie sa budú poskytovať v takej forme, v akej bola podaná žiadosť (písomne/elektronicky/ústne), pokiaľ dotknutá osoba nepožiadala o iný spôsob. Ústne poskytovanie informácií je možné podmieniť preukázaním totožnosti dotknutej osoby. Ak má prevádzkovateľ oprávnené pochybnosti o totožnosti fyzickej osoby, ktorá podáva žiadosť, môže požiadať o poskytnutie dodatočných informácií potrebných na potvrdenie jej totožnosti. Aj pri týchto procesoch je potrebné dbať na bezpečnosť osobných údajov, a v prípade pochybností nereagovať elektronicky na správy bez kvalifikovaného elektronického podpisu. V týchto prípadoch je potom vhodnejšie žiadosti, v ktorých sú sprístupňované osobné údaje, vybaviť písomne do vlastných rúk, aby sa predišlo tomu, že ktorákoľvek anonymná osoba môže vyžiadať chránené údaje o inej osobe.
- III. **Lehotu na vybavenie žiadosti**, ktorá je v zmysle (čl. 12 ods. 3 GDPR a § 29 ods. 3 nového zákona o ochrane osobných údajov) jednomesačná od doručenia žiadosti, vrátane poučenia o tom, kedy a z akých dôvodov je možné lehotu predĺžiť. Umožňuje sa predĺženie lehoty v odôvodnených prípadoch s ohľadom na komplexnosť a počet žiadostí o ďalšie dva mesiace, a to aj opakované. O každom takomto predĺžení musí byť dotknutá osoba informovaná spolu s dôvodmi predĺženia lehoty. Objektívnym dôvodom predĺženia lehoty je napríklad situácia, ak zamestnávateľ vyžiada od dotknutej osoby doplnenie nejakých informácií k posúdeniu a vybaveniu jej žiadosti, pričom doplnenie požadovaných informácií nebude vybavené obratom. Rovnako tak výskyt nejakých bezpečnostných incidentov, ktoré na istý čas paralyzovali informačné systémy zamestnávateľa a pod.
- IV. Transparentnú informáciu **o zavedení a výške poplatkov** za vybavenie žiadostí a poskytnutie informácií. Žiadosti dotknutej osoby a informácie sa primárne vybavujú, resp. poskytujú bezodplatne. Primeraný poplatok zohľadňujúci administratívne náklady možno požadovať za druhú a ďalšiu kópiu dokumentov,

⁶⁶ Podľa čl. 38 ods. 4 GDPR a podľa ust. 45 ods. 4 nového zákona o ochrane osobných údajov dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa tohto zákona.

ktorými zamestnávateľ plní žiadosť dotknutej osoby. Rovnako poplatok možno zaviesť aj za administratívne náklady na vybavenie žiadosti, ktorá je zjavne neopodstatnená alebo neprimeraná, najmä pre jej opakujúcu sa povahu. Zjavnú neopodstatnenosť alebo neprimeranosť žiadosti preukazuje prevádzkovateľ. Opakujúca sa povaha žiadosti je taká, ktorá sa týka tých istých osobných údajov ako aj toho istého uplatňovaného práva. Opakujúcu povahu žiadosti teda nemá žiadosť podaná napríklad k právu na prístup k osobným údajom, a potom žiadosť podaná k právu na výmaz tých údajov, ktorých spracúvanie bolo zistené na základe žiadosti o právo na prístup.

- V. Ďalšie vhodné opatrenia na uplatňovanie práv dotknutej osoby a opatrenia uľahčujúce výkon jej práv podľa okolností konkrétneho prípadu. Napríklad zamestnávateľ môže zadať, či a ako sa prístup k osobným údajom zabezpečí online.

K zodpovednej osobe

Úlohu „prvého kontaktného bodu“ k uplatňovaniu práv dotknutej osobe môže plniť tzv. zodpovedná osoba. Čl. 37 GDPR a v nadväznosti na to ust. § 45 až § 47 nového zákona o ochrane osobných údajov zavádzajú vo vzťahu k určitým prevádzkovateľom i sprostredkovateľom povinnosť ustanoviť zodpovednú osobu. Aj starý zákon o ochrane osobných údajov počítal s nominovaním zodpovednej osoby, ale iba u prevádzkovateľa. Výhoda jej ustanovenia spočívala v tom, že spoločnosť nemusela Úradu oznamovať informačné systémy, v ktorých spracúvali osobné údaje.

GDPR mení podmienky nominácie zodpovednej osoby a viaceré spoločnosti, ktoré doteraz mali zodpovednú osobu, ju už nemusia mať. A naopak, niektorí prevádzkovatelia, ktorí doteraz nemali zodpovednú osobu, i sprostredkovatelia, ju budú musieť určiť. Ostatné subjekty (prevádzkovateľ/sprostredkovateľ/združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov) môžu zodpovednú osobu určiť na dobrovoľnej báze, ak to uznajú za vhodné. Zodpovedná osoba môže potom konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov. Dobrovoľne ustanovená zodpovedná osoba má postavenie a vykonáva svoje úlohy za rovnakých podmienok ako povinne ustanovená osoba.

Samozrejme nič nebráni tomu, aby subjekt, ktorý nemá podľa právnej úpravy povinnosť určiť zodpovednú osobu, a ktorý nechce určiť zodpovednú osobu dobrovoľne, aj tak zamestnal zamestnancov, alebo externých konzultantov a poveril ich úlohami súvisiacimi s ochranou osobných údajov. V takom prípade je dôležité dovnútra spoločnosti, ale najmä vo vzťahoch navonok, odlíšiť funkciu takýchto zamestnancov, alebo externých konzultantov od funkcie zodpovednej osoby.

Kedy zamestnávateľ musí určiť zodpovednú osobu?

Zamestnávateľ musí povinne určiť zodpovednú osobu, ak:

- 1) je orgánom verejnej moci alebo verejnoprávnym subjektom, a to bez ohľadu na to, aké kategórie osobných údajov spracúva a v akej miere (s výnimkou súdov pri výkone ich súdnej právomoci); alebo
- 2) jeho hlavnými činnosťami sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo
- 3) jeho hlavnými činnosťami je spracúvanie citlivých údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky; alebo
- 4) ak to vyžaduje osobitný predpis⁶⁷ alebo medzinárodná zmluva, ktorou je SR viazaná.

Povinnosť ustanoviť zodpovednú osobu v bode 2) a 3) sa viaže na **hlavné činnosti** prevádzkovateľa/sprostredkovateľa, čo sú činnosti, ktoré súvisia s predmetom jeho podnikania. Podľa recitálu 97 GDPR „*v súkromnom sektore sa hlavné činnosti prevádzkovateľa týkajú jeho primárnych činností, a nie spracúvania osobných údajov ako vedľajšej činnosti.*“ Ustanovenie zodpovednej osoby tak nie je povinné pre zamestnávateľa v prípade, keď spracovateľské operácie vykonáva len ako pomocné činnosti k dosiahnutiu základných cieľov svojej činnosti. Napríklad hlavnou činnosťou zamestnávateľa je výkon a realizácia stavebných prác a „len“ podpornou, aj keď nevyhnutnou, činnosťou potrebnou k zabezpečeniu hlavnej činnosti je vedenie evidencie osobných údajov za účelom vyplácania miezd zamestnancom. Takýto zamestnávateľ nie je povinný ustanoviť zodpovednú osobu.

Ďalším kritériom, ktoré sa sleduje pre ustanovenie zodpovednej osoby, je spracúvanie osobných údajov vo **veľkom rozsahu**. Zvažuje sa počet dotknutých osôb, objem spracúvaných osobných údajov, ich rôznorodosť, doba uchovávaní, i geografický rozsah územia, z ktorého spracúvané osobné údaje pochádzajú.

Pokiaľ sa na zamestnávateľa nevzťahuje povinné určenie zodpovednej osoby, odporúča sa vypracovať krátke stanovisko alebo odôvodnenie, prečo sa podmienky GDPR, resp. nového zákona o ochrane osobných údajov pre povinné ustanovenie zodpovednej osoby, nepovažujú za naplnené. Najmä v prípadoch, ak nie je úplne zrejmé, či sú, alebo nie sú podmienky povinného určenia zodpovednej osoby naplnené, takéto stanovisko, resp. odôvodnenie posлuží ako dôkaz, že príslušné faktory na ustanovenie zodpovednej osoby boli zohľadnené a vyhodnotené. Stanovisko, resp. odôvodnenie,

⁶⁷ Momentálne neexistuje osobitný právny predpis, ktorý by prevádzkovateľovi alebo sprostredkovateľovi prikazoval určiť zodpovednú osobu. Inštitút zodpovednej osoby upravuje aj zákon o oznamovaní protispoločenskej činnosti (pozri bližšie kapitolu 4.12). Zodpovedná osoba podľa zákona o protispoločenskej činnosti a zodpovedná osoba podľa zákona o ochrane osobných údajov ale nie sú totožné subjekty. Nie je však vylúčené, aby obidve funkcie vykonávala tá istá osoba.

bude súčasťou vnútropodnikovej dokumentácie a použiteľné pre prípadné kontroly zo strany Úradu.⁶⁸

Zároveň platí, že ak sa na zamestnávateľa vzťahuje povinné určenie zodpovednej osoby, to neznamená, že zodpovednú osobu bude povinný určiť aj jeho sprostredkovateľ a naopak. Podmienky povinného určenia zodpovednej osoby sa sledujú u prevádzkovateľa a sprostredkovateľa samostatne. Ak ide napríklad o zamestnávateľa, ktorý si necháva robiť mzdy svojich zamestnancov externou spoločnosťou, zamestnávateľ nie je povinný určiť zodpovednú osobu. Externá spoločnosť, ktorá vo vzťahu k zamestnávateľovi vystupuje ako sprostredkovateľ a orientuje sa výlučne na spracúvanie miezd pre viacerých zamestnávateľov, t. j. jej hlavnou činnosťou je spracúvanie osobných údajov vo veľkom rozsahu, bude povinná určiť zodpovednú osobu.

Jedna zodpovedná osoba môže fungovať spoločne pre skupinu podnikov, ak zodpovedná osoba bude ľahko dostupná z každej prevádzkárne. „Ľahká dostupnosť“ znamená, že zodpovedná osoba je schopná účinne komunikovať s dotknutými osobami, s každým podnikom a jeho zamestnancami, či s dozornými orgánmi. Zásadná je osobná fyzická dostupnosť zodpovednej osoby, čo zahŕňa možnosť obrátiť sa na ňu telefonicky alebo inými spôsobmi priamej komunikácie.

Kto môže byť zodpovednou osobou?

Je možné, aby zodpovedná osoba

- bola kmeňovým zamestnancom prevádzkovateľa/sprostredkovateľa, alebo
- externe spolupracujúcou osobou, ktorá bude vykonávať svoje úlohy na základe zmluvy o poskytovaní služieb, tzn., že zodpovedná osoba môže byť nielen fyzickou osobou, ale aj právnickou osobou, čo podľa starej právnej úpravy bolo neprípustné.

Konkrétne kvalifikačné požiadavky na zodpovednú osobu nie sú špecifikované. Zodpovedná osoba má disponovať odbornými znalosťami práva a postupov v oblasti ochrany osobných údajov a spôsobilosťou plniť úlohy zodpovednej osoby. Nová právna úprava, na rozdiel od starej právnej úpravy, neustanovuje povinnosť absolvovania skúšky zodpovednej osoby na Úrade.

Aké povinnosti má zamestnávateľ, ak určí zodpovednú osobu?

1) *Povinnosť zverejniť kontaktné údaje zodpovednej osoby a oznámiť ich Úradu.*

Kontaktné údaje zodpovednej osoby by mali obsahovať informácie, ktoré dotknutým osobám a dozorným orgánom umožnia ľahko sa spojiť so zodpovednou osobou (poštová adresa, vyhradené telefónne číslo a/alebo vyhradená e-mailová adresa). Nevyžaduje sa, aby zverejnené kontaktné údaje obsahovali meno zodpovednej osoby. Hoci poskytnutie mena by mohlo byť osvedčeným postupom, rozhodnutie, či je táto

⁶⁸ Spracované podľa Usmernenia WP č. 243 rev.01 týkajúceho sa zodpovedných osôb, ktoré bolo prijaté 13. decembra 2016 a naposledy revidované a prijaté 5. apríla 2017.

informácia za daných okolností potrebná alebo užitočná, záleží na zamestnávateľovi a zodpovednej osobe.

Spôsob zverejnenia ani lehotu, dokedy má zamestnávateľ oznámiť Úradu kontaktné údaje zodpovednej osoby, zákon nešpecifikuje. Odporúča sa zverejnenie a oznámenie vykonať momentom určenia alebo bez zbytočného meškania po ňom. Oznámeniu Úradu podliehajú aj zmeny v kontaktných údajoch zodpovednej osoby.

- 2) *Povinnosť zabezpečiť také podmienky, aby zodpovedná osoba riadne a včas vykonávala všetky činnosti súvisiace s ochranou osobných údajov.*

Odporúča sa, aby zamestnávateľ vybavil zodpovednú osobu dostatočnými kompetenciami a právomocami. Zodpovedná osoba by sa tak mohla zúčastňovať schôdzok vyššieho i stredného manažmentu, včas byť oboznámená s prijímanými rozhodnutiami, ktoré sa môžu týkať ochrany osobných údajov a byť „partnerom na diskusiu“ vo všetkých potenciálnych prípadoch manipulácie s osobnými údajmi.

- 3) *Povinnosť poskytnúť zodpovednej osobe pri plnení jej úloh potrebnú súčinnosť.*

Zamestnávateľ je povinný poskytnúť zodpovednej osobe zdroje potrebné na plnenie jej úloh, zdroje na udržiavanie jej odborných znalostí a samozrejme prístup k osobným údajom a spracovateľským operáciám.

- 4.) *Povinnosť zabezpečiť princíp nezávislosti zodpovednej osoby.*

Zamestnávateľ má zabezpečiť, aby zodpovedná osoba:

- v súvislosti s plnením svojich úloh nedostávala žiadne pokyny, t. j. pokyny, aký výsledok sa má dosiahnuť, ako sa má vyšetrovať sťažnosť, alebo či sa treba radiť s dozorným orgánom a pod.;
- v súvislosti s plnením úloh nebola prepustená alebo sankcionovaná;
- v rámci organizačnej hierarchie spoločnosti bola podriadená priamo vrcholovému riadeniu prevádzkovateľa/sprostredkovateľa.

Aké povinnosti a úlohy má zodpovedná osoba?

Informačná a poradenská činnosť pre zamestnávateľa a jeho zamestnancov, ktorí vykonávajú spracúvanie osobných údajov (t. j. tzv. oprávnené osoby v zmysle dikcie starej právnej úpravy), vrátane vykonávania poradenstva k posúdeniu vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania, ktoré zahŕňa analýzu, kedy je posúdenie vplyvu na ochranu osobných údajov nevyhnutné, zvolenie vhodných metód posúdenia vplyvu, posúdenie záruk, ktoré sa majú aplikovať, aby sa znížilo riziko pre práva a záujmy dotknutých osôb a pod.

Monitoring súladu vnútropodnikových pravidiel na ochranu osobných údajov so všeobecne záväznými právnymi predpismi.

Spolupráca s Úradom a plnenie úloh kontaktného miesta.

Povinnosť v súvislosti s výkonom svojich úloh zachovávať mlčanlivosť a dôvernosť informácií.

IV. Spracúvanie osobných údajov v individuálnych pracovnoprávných vzťahoch (praktické prípady)

4.1 Vyhľadávanie zamestnancov cez sociálne siete

Sociálne siete sú webové služby určené na vytváranie virtuálnych komunít, interakciu medzi nimi, či už v podobe komunikácie, alebo aj zdieľania spoločných dát. Ich rastúca popularita používania vytvára jedinečnú príležitosť ako získať nový zdroj zverejnených informácií, koncentrovaných v zásade na jednom mieste, bez vynaloženia väčších nákladov, pomerne rýchlo a jednoducho. Preto sa sociálne siete začali využívať aj inak, než sa pôvodne predpokladalo. Stali sa reklamným priestorom pre prezentovanie produktov a služieb, ale aj zdrojom pre rôzne prieskumy trhu. Otvorene sa k ich využívaniu hlásia aj personalisti a zamestnávateľia.⁶⁹ Užívateľské profily totiž poskytujú dostatok osobných a behaviorálnych údajov, ktoré môžu byť využité pri výbere vhodných zamestnancov. Potenciál využitia sociálnych sietí ako nástroja výberu ľudských zdrojov bol pritom vytvorený v dôsledku nie celkom rozumného správania sa ich používateľov. Na internete sú zverejňované nielen bežné osobné údaje, ale aj citlivé informácie o národnosti, rasovej, politickej príslušnosti, zdravotnom stave i intímnom živote, ktoré v súhrne vytvárajú ľahko vystopovateľnú digitálnu identitu. Aj keď používatelia sociálnych sietí môžu kontrolovať, čo verejne sprístupnia, strácajú kontrolu nad tým, ako so zverejnenou informáciou naloží jej príjemca.⁷⁰

Určitý obraz o potenciálnom zamestnancovi potom dotvárajú aj ďalšie informácie; napríklad komentáre, príspevky v tzv. blogoch, fotografie a členstvá v skupinách. Komentáre k udalostiam, či fotografiám „na nástenkách“ priateľov majú transparentnejšiu výpovednú hodnotu ako životopis či motivačný list, v ktorom sa uchádzač o zamestnanie snaží (neraz umelo) vykresliť sám seba v čo najlepšom svetle. Obraz o užívateľovi sociálnej siete potom dokresľuje aj to, čo o ňom na sociálnej sieti „povedia“ jeho priatelia. Personalisti potvrdzujú, že na základe internetovej (digitálnej) stopy môže byť fyzická osoba pozvaná na pracovný pohovor, či dokonca prijatá do zamestnania, ale takisto odmietnutá, či zbytočne znevýhodnená, aj keď sa neskôr môže ukázať, že uvádzané informácie boli skreslené, či dokonca nepravdivé.⁷¹ K negatívnym faktorom najviac znižujúcim profesijný vzhlad uchádzača o zamestnanie patria: nízka pravopisná úroveň komunikácie na sociálnych sieťach, zverejnené provokatívne fotografie, prezentácia nepatričného životného štýlu (alkoholizmus, ľahké drogy), agresívne a iné nevhodné pripomienky.

Vyhľadávanie potenciálnych zamestnancov cez sociálne siete a monitoring ich správania sa na internete má svoje dosahy aj do oblasti práva osobných údajov. GDPR

69 HVOZDOVIČOVÁ, J.: Personálne agentúry hľadajú ľudí aj na Facebooku. Dostupné na:

<http://ekonomika.sme.sk/c/5869601/personalne-agentury-hladaju-ludi-aj-na-facebooku.html>.

70 LUKIČ, Ľ. – SOKOL, P.: (Ne)bezpečie sociálnych sietí; prvé vydanie, vydalo European Information Society Institute, o. z., v roku 2014, s. 9, ISBN 978-80-971307-2-5. Dostupné na:

http://www.eisionline.org/files/nebezpecenstvo_socialnych%20sieti.pdf

71 BÖHMOVÁ, L. – PAVLÍČEK, A.: Personalistika a budoucnost sociálních sítí v ČR; in: Scientific Papers of the University of Pardubice. Series D, Faculty of Economics & Administration, 2013, roč. 20, č. 27, s. 14 – 22.

a nový zákon o ochrane osobných údajov posilňujú generálne práva dotknutých osôb a explicitne poskytujú ochranu potenciálnym uchádzačom o zamestnanie v prípadoch, ak sa zamestnávateľ rozhodne pracovné miesta obsadzovať využitím skríningu ich digitálnej identity. Ak personalista spracúva osobné údaje potenciálnych uchádzačov o zamestnanie tým spôsobom, že tieto vyhľadáva na internete, používa ako vstupné údaje do aplikácie, ktorá mu zostaví zoznam vhodných uchádzačov a následne pre nich generuje pozvánky na pracovný pohovor, ide o spracovateľskú operáciu, ktorá napĺňa znaky profilovania (vysvetlené v kapitole 3.3.8). Potom je potrebné na zreteľ vziať tieto zákonné pravidlá:

- i) Pred vznikom pracovného pomeru môže zamestnávateľ vyžadovať od fyzickej osoby, ktorá sa uchádza o zamestnanie, len také údaje, ktoré súvisia s prácou, ktorú má vykonávať (ust. § 41 ods. 5 Zákonník práce). Rámcovo ďalej ustanovenie § 41 ods. 6 Zákonníka práce zakazuje zamestnávateľovi vyžadovať od fyzickej osoby uchádzajúcej sa o zamestnanie informácie o tehotenstve, rodinných pomeroch, o bezúhonnosti (s určitou výnimkou), o politickej, odborovej a náboženskej príslušnosti. Uvedené je potrebné vykladať tak, že tieto informácie si nemôže zamestnávateľ zaobstarávať ani sám, ani prostredníctvom tretej osoby, a preto tieto osobné údaje nemôžu ani vstupovať ako údaje do profilovania.
- ii) V súlade s ustanovením § 10 ods. 3 písm. e) starého zákona o ochrane osobných údajov platilo, že na spracúvanie osobných údajov, ktoré už boli zverejnené v súlade so zákonom a prevádzkovateľ ich náležite označil za zverejnené, nebol potrebný súhlas dotknutej osoby. Za osobné údaje zverejnené v súlade so zákonom bolo možné považovať osobné údaje, ktoré o sebe zverejnili samotné dotknuté osoby.⁷² Spracovateľskej operácii v podobe skríningu digitálnej identity na účely vyhľadávania vhodného zamestnanca tak prislúchal tento (aj keď podľa nášho názoru nie celkom bezproblémovo)⁷³ právny základ. GDPR a nový zákon o ochrane osobných údajov však s takýmto právnym základom spracúvania všeobecných (bežných) osobných údajov už ďalej nepočítajú (viď zrušené právne základy, kapitola 2.3.2.) a ani tomuto právnemu základu nevytvárajú ekvivalent. Každý účel spracúvania osobných údajov musí mať svoj právny základ, čo platí aj pre spracúvanie takých osobných údajov, ktoré už boli zverejnené, či už vo verejných registroch alebo samotnými dotknutými osobami.⁷⁴ Zverejnené osobné

72 MATEJKA, J.: Internet jako objekt práva: hledání rovnováhy autonomie a soukromí; 1. vydanie, Praha: CZ.NIC, 2013, s. 100 a nasl., ISBN 978-80-904248-7-6.

73 K tomu: ŽULOVÁ, J.: Používanie sociálnych sietí pri výbere zamestnancov (z pracovnoprávneho hľadiska); Justičná revue, 68, 2016, č. 6-7, s. 729 – 736.

74 Paradoxne k celej situácii nám však vyznieva výnimka zo spracúvania citlivých osobných údajov uvedená v čl. 9 ods. 2 písm. e) GDPR a ust. 16 ods. 2 písm. e) nového zákona o ochrane osobných údajov. Spracúvanie citlivých osobných údajov sa všeobecne zakazuje, pokiaľ sa neuplatní niektorá z výnimiek, medzi ktoré je zaradené spracúvanie takých osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila. Aj keď aplikácia citovaného ustanovenia na pracovnoprávne vzťahy si žiada podrobnejší rozbor, sme toho názoru, že momentálne postačuje odkázať na nemožnosť zamestnávateľa vziať na účely profilovania také na internete zverejnené citlivé osobné údaje, ktorých spracúvanie je zakázané podľa ust. § 41 ods. 6 Zákonníka práce.

údaje nemožno neobmedzenie preberať a spracúvať a tým na nich profitovať. Osobné údaje patria dotknutým osobám a patrí im aj právo, aby naďalej rozhodovali, ako sa s ich zverejnenými údajmi naloží pri ďalších spracovateľských operáciách. Verejnosť osobných údajov *a priori* neznamená možnosť ich ďalšieho neobmedzeného spracúvania. K profilovaniu preto potrebuje personalista niektorý z právnych základov uvedených v čl. 6 ods. 1 GDPR alebo ust. § 13 ods. 1 nového zákona o ochrane osobných údajov (bližšie kapitola 2.3.2).

- iii) Práva dotknutej osoby v pozícii potenciálneho uchádzača o zamestnanie, ktorý je profilovaný, sú ďalej posilnené predovšetkým cez inovovanú informačnú povinnosť prevádzkovateľa. Ak personalista uskutočňuje profilovanie na základe osobných údajov, v súlade s článkom 13 a 14 GDPR a ust. § 19 a 20 nového zákona o ochrane osobných údajov, by mal jednotlivé osoby informovať o tom, že využíva profilovanie (prípadne aj automatizované rozhodovanie), jasne a jednoducho im vysvetliť, ako celý tento proces funguje a aké to môže mať pre nich dôsledky. V prípade, že nezískava osobné údaje priamo od dotknutej osoby, je povinný ju podľa článku 14 ods. 2 písm. f) GDPR a § 20 ods. 2 písm. f) nového zákona o ochrane osobných údajov informovať o zdroji, z ktorého pochádzajú jej osobné údaje, prípadne podať jej informácie o tom, či osobné údaje pochádzajú z verejne prístupných zdrojov (napr. sociálne siete, registre a pod.). Samostatne by mal personalista uviesť informáciu o práve dotknutej osoby vzniesť námietku proti procesu profilovania, i o práve namietať správnosť a aktuálnosť osobných údajov vstupujúcich do profilovania. Právo na opravu dotknutej osoby nevyklučuje ani žiadosť o opravu „výstupných“ údajov.⁷⁵ Plnenie informačnej povinnosti sa pritom musí uskutočniť pri prvej komunikácii s uchádzačom alebo do jedného mesiaca od získania takýchto údajov, a to aj v prípade neprijatia uchádzača (bližšie kapitola 3.3.1. Právo na informácie).
- iv) Ak sa zamestnávateľ rozhodne na skríning digitálnej identity a profilovanie potenciálnych uchádzačov o zamestnanie využiť externého dodávateľa, nie svojho vlastného zamestnanca, je potrebné kvalifikovane posúdiť aj vzájomný právny vzťah medzi zamestnávateľom a týmto externým subjektom.

Zamestnávateľ je v kontexte ochrany osobných údajov zamestnanca **prevádzkovateľom**. Prevádzkovateľom je každý, u koho si môžu dotknuté osoby uplatniť svoje práva v praxi a teda ten:

1. kto sám alebo spoločne s inými určí účel a prostriedky spracúvania osobných údajov a ktorý spracúva osobné údaje vo vlastnom mene; alebo
2. komu funkcia prevádzkovateľa vyplýva zo zákona, alebo kto splní zákonom stanovené požiadavky na určenie statusu prevádzkovateľa (ak osobitný predpis verejným alebo súkromným subjektom ukladá povinnosť spracúvať určité údaje).

⁷⁵ K práve namietať pozri kapitolu 3.3.7, k práve na opravu kapitolu 3.3.3.

Ak dvaja, alebo viacerí prevádzkovatelia, spoločne určia účely a prostriedky spracúvania, sú **spoločnými prevádzkovateľmi**. GDPR upravuje vzájomný vzťah spoločných prevádzkovateľov a diktuje náležitosti ich zmluvného vzťahu. Ak si zamestnávateľ najme spoločnosť, ktorá mu má pomôcť s profilovaním potenciálnych zamestnancov, a to takým spôsobom, že spoločná databáza vhodných kandidátov sa vytvorí zo vstupných údajov, ktoré požaduje u potenciálnych kandidátov sledovať zamestnávateľ, ale súčasne aj zo vstupných údajov, ktoré navrhne sledovať externý dodávateľ, pretože podľa svojich skúseností vie, že tieto údaje môžu byť pre nájdenie vhodného zamestnanca relevantné, máme za to, že vzťah zamestnávateľa a spoločnosti je potrebné klasifikovať ako vzťah spoločných prevádzkovateľov. V praxi sa zamestnávatelia uchýľujú skôr k uzavretiu sprostredkovateľskej zmluvy, čo podľa nášho názoru nie je správna kvalifikácia právneho vzťahu, keďže zamestnávateľ i spoločnosť spoločne kontrolujú účel spracúvania a sčasti majú spoločné i prostriedky spracúvania v spoločnom súbore operácií.

Spoloční prevádzkovatelia sú povinní podľa GDPR uzavrieť **vzájomnú dohodu** (ak ich vzájomný vzťah nie je upravený osobitným predpisom), v ktorej:

- transparentne určia príslušné zodpovednostné vzťahy (s dôrazom na práva dotknutej osoby a plnenie informačnej povinnosti);
- určia kontaktné miesto pre dotknutú osobu (odporúča sa kontaktné miesto jedného prevádzkovateľa) a
- poskytnú základné časti ich vzájomnej dohody dotknutým osobám.

Bez ohľadu na rozdelenie zodpovednosti spoločnými prevádzkovateľmi vo vzájomnej dohode, dotknutá osoba má právo uplatniť svoje právo u každého prevádzkovateľa a svoj nárok voči každému prevádzkovateľovi.

Zamestnávateľ nie je povinný spracúvať osobné údaje sám, ale môže spracúvaním osobných údajov poveriť externý subjekt – **sprostredkovateľa**. Je zodpovednosťou prevádzkovateľa poveriť len sprostredkovateľa poskytujúceho dostatočné záruky na to, že sa prijímú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo zákonné požiadavky, a aby sa zabezpečila ochrana práv dotknutej osoby.

Sprostredkovateľ:

- je fyzická osoba alebo právnická osoba, orgán verejnej moci, iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa;
- účel spracúvania si nikdy neurčuje sám, ale určí mu ho prevádzkovateľ (ak sprostredkovateľ určí účely a prostriedky spracúvania, považuje sa v súvislosti s daným spracúvaním za prevádzkovateľa);
- vždy ide o samostatný (externý) subjekt vo vzťahu k prevádzkovateľovi (sprostredkovateľom nie je zamestnanec oprávnený spracúvať osobné údaje pod priamym dohľadom zamestnávateľa);
- so súhlasom prevádzkovateľa môže poveriť spracúvaním osobných údajov ďalšieho sprostredkovateľa (terminológiou starého zákona o ochrane osobných

údajov **tzv. subdodávateľ**, nový zákon o ochrane osobných údajov pod vplyvom GDPR tento pojem nepreberá);

- za spracúvanie osobných údajov sprostredkovateľom zodpovedá prevádzkovateľ, zodpovednosť voči prevádzkovateľovi za subdodávateľa nesie sprostredkovateľ.

GDPR ustanovuje nové a rozširuje pôvodné obsahové náležitosti zmluvy medzi prevádzkovateľom a sprostredkovateľom. Zmluva musí obsahovať:

- a) predmet a dobu spracúvania;
- b) povahu a účel spracúvania;
- c) zoznam alebo rozsah osobných údajov;
- d) kategórie dotknutých osôb;
- e) povinnosti a práva prevádzkovateľa;

GDPR a nový zákon o ochrane osobných údajov konkretizujú a zdôrazňujú niektoré povinnosti sprostredkovateľa, na ktoré je nevyhnutné v zmluve medzi prevádzkovateľom a sprostredkovateľom pamätať. Sprostredkovateľ:

- a) spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa;
- b) poučí osoby oprávnené spracúvať osobné údaje o povinnosti zachovávať mlčanlivosť a dôvernosc informácií;
- c) vykoná všetky opatrenia na zabezpečenie bezpečnosti spracúvania;
- d) dodrží podmienky zapojenia ďalšieho sprostredkovateľa (subdodávateľa);
- e) poskytne prevádzkovateľovi potrebnú súčinnosť v súvislostiach so zabezpečením práv dotknutej osoby, s prijatím opatrení na zabezpečenie bezpečnosti spracúvania a v súvislosti s kontrolou plnenia povinností;
- f) zlikviduje, alebo vráti osobné údaje po ukončení služby prevádzkovateľovi.

Podľa okolností konkrétneho prípadu tak medzi zamestnávateľom, ktorý si najme externý subjekt na profilovanie zamestnancov, môže ísť o vzájomný vzťah dvoch spoločných prevádzkovateľov (viď vyššie) alebo o vzťah prevádzkovateľa a sprostredkovateľa. Ak externá spoločnosť vytvorí profilovaním databázu vhodných kandidátov podľa pokynov a na účely vyžadované zamestnávateľom, no na svoju činnosť databázu v nijakom smere využívať nebude, je vzťah zamestnávateľa a externej spoločnosti vzťahom prevádzkovateľa a sprostredkovateľa.

4.2 Spracúvanie osobných údajov v životopisoch a vytváranie databáz z životopisov

K spracúvaniu osobných údajov v pracovnoprávných vzťahoch prichádza už vo fáze pred založením samotného pracovného pomeru, alebo pracovnoprávného vzťahu, na základe niektorej z dohôd o prácach vykonávaných mimo pracovného pomeru. V zmysle § 41 Zákonníka práce ide o tzv. predzmluvné vzťahy, ktorých účelom je zhro-

maždiť určitý súhrn informácií (vrátane osobných údajov) o potenciálnych zamestnancoch na uľahčenie rozhodovacieho procesu zamestnávateľa.

V rámci predzmluvných vzťahov prichádza do úvahy spracúvanie osobných údajov na týchto právnych základoch:

- na základe súhlasu dotknutej osoby podľa čl. 6 ods. 1 písm. a) GDPR a ust. § 13 ods. 1 písm. a) nového zákona o ochrane osobných údajov (na základe súhlasu uchádzača o zamestnanie sa spracúvajú osobné údaje uvedené v doručenom životopise);
- spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby podľa čl. 6 ods. 1 písm. b) GDPR a ust. § 13 ods. 1 písm. b) nového zákona o ochrane osobných údajov (na tomto právnom základe prebieha spracúvanie osobných údajov pri uskutočňovaní pracovného pohovoru, alebo výberového konania);
- spracúvanie osobných údajov je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná podľa čl. 6 ods. 1 písm. c) GDPR a ust. § 13 ods. 1 písm. c) nového zákona o ochrane osobných údajov (ide o spracúvanie všetkých tých osobných údajov, ktoré potrebuje zamestnávateľ na to, aby nahlásil zamestnanca do Sociálnej poisťovne, zdravotnej poisťovne, na účely vedenia mzdového listu a pod.).

Prvý kontakt s osobnými údajmi uchádzača o zamestnanie spravidla predstavuje doručenie životopisu. Zamestnávateľ môže získavať osobné údaje zo životopisov, ktorými uchádzači reagujú na konkrétnu pracovnú pozíciu alebo zo životopisov, ktoré zasielajú fyzické osoby potenciálnemu zamestnávateľovi, pričom nereagujú na konkrétnu pracovnú pozíciu. Osobné údaje obsiahnuté v životopise, ktorý zašle uchádzač zamestnávateľovi, spracúva zamestnávateľ na základe súhlasu dotknutej osoby. Súhlas je vyjadrený úkonom dotknutej osoby, ktorá z vlastnej vôle zaslala životopis, pričom je možné predpokladať, že ho zaslala s cieľom získať prácu.⁷⁶

Ak zamestnávateľ na inzerovanie voľných pracovných ponúk využíva vlastnú webovú stránku (spravidla osobitne vytvorená sekcia ponuky práce, ponuka voľných pracovných miest a pod.), ponúka sa mu vhodný a vlastný priestor, aby reguloval zoznam osobných údajov, ktoré od potenciálneho uchádzača potrebuje. Zostavením dotazníka, ktorý uchádzač vyplní, tak môže predchádzať situácii, kedy uchádzač uvedie aj tzv. zakázané osobné údaje (napr. § 41 ods. 6 Zákonníka práce).

V prípade, že uchádzač doručil zamestnávateľovi životopis, ktorý obsahoval informácie z kategórie tzv. zakázaných osobných údajov (vydatá, bezdetná, národnosť slovenská a pod.) a zamestnávateľ nemal v úmysle ďalej tieto údaje systematicky spracúvať, išlo v zmysle starej právnej úpravy o tzv. náhodne získané údaje a platilo ust. § 3 ods. 2

76 ŠVEC, M., VALENTOVÁ, T. Ochrana osobných údajov v pracovnoprávných vzťahoch. Bratislava: Wolters Kluwer, 2016, s. 60.

písm. b) starého zákona o ochrane osobných údajov: *Tento zákon sa nevzťahuje na osobné údaje, ktoré boli získané náhodne bez predchádzajúceho určenia účelu a prostriedkov spracúvania, bez zámeru ich ďalšieho spracúvania v usporiadanom systéme podľa osobitných kritérií a nie sú ďalej systematicky spracúvané.* Aj keď obdobné ustanovenie GDPR nepozná a nový zákon o ochrane osobných údajov tiež také ustanovenie nepreberá, opatrenia a úsilie, ktoré musel a musí zamestnávateľ vyvinúť sú totožné. Je povinnosťou zamestnávateľa prijať také primerané opatrenia, aby zabezpečil, že takto získané zakázané osobné údaje sa nestanú súčasťou informačného systému osobných údajov. V praxi to znamená, že je povinný vo svojich podmienkach nastaviť mechanizmus, ktorým zabezpečí anonymizáciu týchto osobných údajov (napr. ich začiatenie), alebo iným vhodným spôsobom zabezpečiť, že sa tieto osobné údaje nestanú súčasťou informačného systému osobných údajov.

V podmienkach zamestnávateľov pracujúcich s veľkým množstvom dát (životopisov) sa môže mechanický spôsob anonymizácie javiť ako personálne náročné. Z hľadiska procesu výberu uchádzača v súlade so Zákonníkom práce však nie je možné vylúčiť uchádzača, ktorý zaslal takéto tzv. zakázané osobné údaje, z výberu. Zamestnávateľ by mal zabezpečiť, aby v procese samotného výberu zamedzil k tzv. zakázaným osobným údajom prístup zamestnancom, ktorí o výbere uchádzača rozhodujú [napr. personálne pracovisko predloží „výberovej komisii“ súhrn nevyhnutných údajov (okrem tzv. zakázaných osobných údajov), ktoré potrebuje na výber uchádzača]. Po ukončení výberu musí zamestnávateľ zabezpečiť bezodkladnú likvidáciu alebo vrátenie životopisu s tzv. zakázanými osobnými údajmi uchádzačovi.

Vytvorenie „sekcie, záložky“ s ponukou práce na vlastnom webovom sídle zamestnávateľa mu ponúka možnosť právneho ošetrenia ďalšej spracovateľskej operácie so životopismi uchádzačov. Zamestnávateľ si vietýmto spôsobom vyžiadať súhlas uchádzača o zamestnanie na ďalší účel spracúvania jeho osobných údajov uvedených v životopise, a to na zaradenie zaslaného životopisu do databázy a jeho využiteľnosti v prípade, ak sa pre uchádzača naskytne iná vhodná práca. Na vedenie takéhoto informačného systému platia všetky zákonné pravidlá ochrany osobných údajov, vrátane zásad spracúvania osobných údajov. Pozornosť je potrebné upriamiť na:

- *získanie súhlasu* - zamestnávateľ môže zhromažďovať doručené životopisy vo vlastnej databáze na účely neskoršej realizácie výberových konaní výlučne na základe súhlasu uchádzača o zamestnanie;
- *aktualizáciu osobných údajov* – podľa zásady správnosti majú byť spracúvané osobné údaje správne a podľa potreby aktualizované;
- *stanovenie doby uchovávania životopisov* - za primeranú lehotu na spracúvanie osobných údajov v databáze uchádzačov je spravídla možné považovať 6 mesiacov až 1 rok;⁷⁷

⁷⁷ Spracúvanie osobných údajov v databáze životopisov po dlhšiu dobu je primerané u sprostredkovateľov práce a v agentúrnom zamestnávaní. K tomu: ŠVEC, M., VALENTOVÁ, T. Ochrana osobných údajov v pracovnoprávných vzťahoch. Bratislava: Wolters Kluwer, 2016.

- *na likvidáciu alebo vrátenie životopisu* - ak zamestnávateľ nezíska, alebo nemá súhlas uchádzača o zamestnanie so zaradením jeho životopisu do databázy, ak pominula primeraná doba uchovávanía životopisu, alebo ak pominul účel takéhoto spracúvania, je zamestnávateľ povinný doručený životopis vrátiť, alebo získané osobné údaje zlikvidovať.

4.3 Pracovný pohovor z pohľadu ochrany osobných údajov

Výber vhodného uchádzača na pracovnú pozíciu je z hľadiska práva osobných údajov procesom, v ktorom dochádza k spracúvaniu všeobecných i citlivých osobných údajov o uchádzačoch o zamestnanie (napr. údaje o zdravotnej alebo psychickej spôsobilosti na výkon práce, údaje o zdravotnom postihnutí pri realizácii tzv. kvóta systému,⁷⁸ informácie o bezúhonnosti z výpisu z registra trestov).

Rozsah spracúvaných osobných údajov pri výberovom konaní sa líši s ohľadom na pracovnú pozíciu, pre obsadenie ktorej sa realizuje výberové konanie, t. j. v závislosti od požiadaviek na riadny výkon dohodnutej práce určených zamestnávateľom vo vnútornom predpise, alebo v závislosti od predpokladov ustanovených právnymi predpismi na výkon dohodnutej práce. Svojvoľné určenie rozsahu spracúvaných osobných údajov v procese výberu vhodného zamestnanca neprichádza do úvahy a rozsah spracúvaných osobných údajov je limitovaný:

- čl. 11 Zákonníka práce, podľa ktorého *zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva, alebo vykonával.*
- zákazom diskriminácie; uchádzač o zamestnanie má právo na prístup k zamestnaniu, ktoré sa má uplatňovať bez akýchkoľvek obmedzení v súlade so zásadou rovnakého zaobchádzania v pracovnoprávných vzťahoch a obdobných právnych vzťahoch, a preto zamestnávateľ nesmie zhromažďovať o uchádzačovi také informácie, ktoré by ho v samotnom výberovom konaní znevýhodnili oproti ostatným.
- ust. § 41 ods. 5 Zákonníka práce, ktoré v pozitívnom vyjadrení dovoľuje zamestnávateľovi žiadať od fyzickej osoby, ktorá sa uchádza o prvé zamestnanie, len informácie, ktoré súvisia s prácou, ktorú má vykonávať, pričom od fyzickej osoby, ktorá už bola zamestnávaná, môže požadovať predloženie pracovného posudku a potvrdenia o zamestnaní. Pri získavaní a poskytovaní pracovného posudku platí, že zamestnávateľ nesmie poskytnúť informácie o svojom bývalom zamest-

⁷⁸ Podľa § 63 ods. 1 písm. d) zákona o službách zamestnanosti je zamestnávateľ povinný zamestnávať občanov so zdravotným postihnutím, ak zamestnáva najmenej 20 zamestnancov a ak úrad práce, sociálnych vecí a rodiny v evidencii uchádzačov o zamestnanie vedie občanov so zdravotným postihnutím v počte, ktorý predstavuje 3,2 % z celkového počtu jeho zamestnancov. Bližšie ku kvóta systému: DOLOBÁČ, M. Kvóta systém v pracovnom práve. In: Diskriminácia v zmluvnom práve: 3. december 2014, Trnava. Bratislava: Typi Universitatis Tyrnaviensis, 2015, s. 111-120. ISBN9788080828356.

nancovi bez jeho súhlasu, resp. informácie poskytuje len na žiadosť zamestnanca. Zamestnávateľ, ktorý obsadzuje voľnú pozíciu, môže informácie o uchádzačovi súvisiace s jeho predchádzajúcimi skúsenosťami získať výlučne od zamestnanca alebo len prostredníctvom neho od tretích subjektov (napr. od predchádzajúceho zamestnávateľa). Zamestnávateľ môže požiadať uchádzača o predloženie referencií a kontaktných údajov osôb, ktoré môžu tieto referencie potvrdiť. Tieto kontaktné osoby však musia disponovať hodnoverne preukázateľným súhlasom dotknutej osoby (uchádzača o zamestnanie), aké informácie o nej môžu poskytnúť (zoznam/rozsah osobných údajov) a komu ich môžu poskytnúť.

- ust. § 41 ods. 6 Zákonníka práce, ktoré v negatívnom vymedzení zakazuje zamestnávateľovi vyžadovať od fyzickej osoby informácie o tehotenstve, rodinných pomeroch, bezúhonnosti s výnimkou, ak ide o prácu, pri ktorej sa podľa osobitného predpisu vyžaduje bezúhonnosť, alebo ak požiadavku bezúhonnosti vyžaduje povaha práce, ktorú má fyzická osoba vykonávať, o politickej príslušnosti, odborovej príslušnosti a náboženskej príslušnosti.
- ust. § 62 ods. 3 zákona č. 5/2004 Z. z. o službách zamestnanosti v znení neskorších predpisov, podľa ktorého zamestnávateľ nesmie pri výbere zamestnanca vyžadovať informácie, ktoré sa týkajú národnosti, rasového pôvodu alebo etnického pôvodu, politických postojov, členstva v odborových organizáciách, náboženstva, sexuálnej orientácie, informácie, ktoré odporujú dobrým mravom, a osobné údaje, ktoré nie sú potrebné na plnenie povinností zamestnávateľa ustanovených osobitným predpisom. Zamestnávateľ je pritom povinný na požiadanie občana preukázať nutnosť vyžadovaného osobného údajaja.

S odkazom na znenie § 41 ods. 2 Zákonníka práce možno uviesť, že rovnako, ako v prípade požiadavky na bezúhonnosť, tak i v prípade vyžadovanej zdravotnej spôsobilosti na prácu, alebo psychickej spôsobilosti na prácu, resp. iného predpokladu, sa môže rozsah informácie zamestnávateľa orientovať len na výsledok takéhoto posúdenia, t. j. či fyzická osoba je, alebo nie je spôsobilá na danú prácu z hľadiska zdravotnej alebo psychickej spôsobilosti. Zamestnávateľ ale nemá (nesmie) disponovať informáciami o priebehu a podrobnostiach tohto posudzovania, s ohľadom napr. na detailný popis zdravotného stavu fyzickej osoby.

Jedným zo spôsobov posudzovania schopností uchádzačov sú **psychotesty**. Psychotesty umožňujú získať o uchádzačovi aj také informácie, ktoré by sám osebe neprezradil, umožňujú získať informácie o mentálnej úrovni uchádzača, o jeho osobnosti, schopnosti pracovať pod tlakom a pod. Osobné údaje (informácie o uchádzačovi) získané na základe psychotestov patria do kategórie citlivých osobných údajov. Na ich spracúvanie sa vyžaduje jeden z právnych základov uvedených v čl. 9 ods. 2 GDPR a ust. § 16 ods. 2 nového zákona o ochrane osobných údajov. V prípade, že je účelom absolvovania psychotestu zistenie psychickej spôsobilosti na prácu, ktorú ako predpoklad na výkon práce vyžaduje osobitný právny predpis, využiteľný je právny základ uvedený v čl. 9

ods. 2 GDPR a ust. § 16 ods. 2 písm. b) nového zákona o ochrane osobných údajov.⁷⁹ V prípade, že osobitný právny predpis neustanovuje na výkon práce predpoklad psychickej spôsobilosti, zamestnávateľ potrebuje výslovný súhlas uchádzača o zamestnanie s takýmto spracúvaním osobných údajov (čl. 9 ods. 2 písm. a) GDPR a ust. § 16 ods. 2 písm. a) nového zákona o ochrane osobných údajov).⁸⁰

Pri využívaní psychotestov, ako prostriedku pre zisťovanie psychickej spôsobilosti uchádzača, je potrebné mať na zreteli, že psychotesty samy osebe sú len jednou z metód využívaných pri psychodiagnostike. Preto je dôležité zvážiť ich potrebu a poskytnúť dostatočné množstvo relevantných informácií súvisiacich s obsadzovaným miestom psychológovi, alebo inej osobe oprávnenej vykonávať posudzovanie psychickej pracovnej spôsobilosti, s cieľom zabezpečiť relevantný výsledok. Psychická pracovná spôsobilosť sa môže zisťovať rôznymi testami zameranými na jednotlivé schopnosti, danosti uchádzača. Najčastejšie sú využívané testy inteligencie, ktorými sa zisťujú určité špecifické schopnosti uchádzača, spravidla prostredníctvom výkonových alebo manipulačných testov. Ďalším typom sú testy osobnosti, ktoré mapujú osobnosť človeka, môžu sa orientovať na silné/slabé stránky osobnosti, schopnosť interakcie alebo testy špecifických funkcií, ktorými sa zisťuje napr. schopnosť sústrediť sa, alebo pamäť.

Nadalej platí, že psychotesty môže vykonávať len psychológ alebo ten, komu to umožňuje osobitný zákon, t. j. poskytovateľ zdravotnej starostlivosti alebo osoba vykonávajúca služby súvisiace s poskytovaním zdravotnej starostlivosti a v jej mene odborne spôsobilá oprávnená osoba, ktorá je viazaná povinnosťou mlčanlivosti o skutočnostiach, o ktorých sa dozvedela pri výkone svojej činnosti a povinnosťou dodržiavať zásady profesijnej etiky (napr. § 33 zákona o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov). Ešte raz pripomíname, že zamestnávateľ je na účely overenia psychickej pracovnej spôsobilosti oprávnený spracúvať **len výsledok psychotestov v rozsahu, či uchádzač je, alebo nie je vhodný na danú pracovnú pozíciu.**

Pred samotnou realizáciou pracovného pohovoru je potrebné voči uchádzačom o zamestnanie splniť informačnú povinnosť (viď právo dotknutej osoby na informácie, bližšie kapitola 3.3.1.). Uvedené platí o to viac, že GDPR a nový zákon o ochrane osobných údajov informačnú povinnosť prevádzkovateľa rozšíril na všetky právne tituly, na základe ktorých sa osobné údaje spracúvajú. Podľa starého zákona o ochrane osobných údajov sa výnimka z poskytnutia informácií podľa § 15 ods. 1 starého zákona o ochrane osobných údajov vzťahovala na každého, kto spracúval osobné údaje dotknutých osôb

79 Spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná alebo podľa kolektívnej zmluvy, ak poskytujú primerané záruky ochrany základných práv a záujmov dotknutej osoby.

80 K tomu, či zamestnávateľ môže vôbec vyžadovať od uchádzača, aby sa podrobil psychotestom pozri kapitolu 4.4.

na základe osobitného zákona, t. j. bez súhlasu dotknutej osoby. Od účinnosti GDPR a nového zákona o ochrane osobných údajov informačnú povinnosť nie je potrebné plniť v takom rozsahu, v akom dotknutá osoba už dané informácie má, či v rozsahu, v akom sa získanie týchto informácií alebo poskytnutie týchto informácií ustanovuje v osobitnom predpise, ktorý sa na prevádzkovateľa vzťahuje a v ktorom sú ustanovené primerané opatrenia na ochranu práv a oprávnených záujmov dotknutej osoby.

Po skončení pracovného pohovoru zamestnávateľ disponuje súborom rôznych informácií, ktoré v priebehu výberu získal (napr. životopis, rôzne čestné vyhlásenia, potvrdenie o zdravotnom stave, informácia o psychickej pracovnej spôsobilosti, testy odbornej spôsobilosti a pod.). V prípade úspešných uchádzačov sa tieto informácie stávajú súčasťou personálnej zložky zamestnanca. V prípade neúspešných uchádzačov je zamestnávateľ povinný postupovať v súlade s prijatými primeranými bezpečnostnými opatreniami a zavedenými mechanizmami s cieľom osobné údaje bezodkladne likvidovať po skončení účelu ich spracúvania. Originály alebo overené fotokópie dokumentov by mal zamestnávateľ uchádzačovi bezodkladne vrátiť. Ostatné dokumenty zlikvidovať spôsobom, ktorý zaručí primeranú ochranu a bezpečnosť spracúvaných osobných údajov. Zamestnávateľ je oprávnený uchovávať osobné údaje o uchádzačovi v rozsahu informácií nevyhnutných pre dokumentovanie priebehu výberu a jeho výsledku. V prípade, že zamestnávateľ získal súhlas dotknutej osoby (neúspešný uchádzač o zamestnanie) na zaradenie jej osobných údajov do databázy uchádzačov, je oprávnený osobné údaje v rozsahu životopisu ďalej spracúvať v tejto databáze.

4.4 Zisťovanie zdravotnej a psychickej spôsobilosti uchádzačov o zamestnanie

Zamestnávateľ môže podľa § 41 ods. 2 Zákonníka práce vyžadovať informácie týkajúce sa zdravotnej alebo psychickej spôsobilosti, prípadne iného predpokladu na výkon práce od budúceho zamestnanca len vtedy, ak sa na daný výkon práce takáto spôsobilosť vyžaduje podľa osobitného zákona. Ak určitý druh práce teda vyžaduje osobitnú spôsobilosť budúceho zamestnanca, zamestnávateľ smie uzatvoriť pracovný pomer len s osobou, ktorá tento osobitný predpoklad spĺňa. **Zisťovanie zdravotného stavu budúceho zamestnanca, ako aj zisťovanie jeho psychickej spôsobilosti na výkon určitého druhu práce smeruje k tomu, aby zamestnávateľ mal preukázané, či zamestnanec je spôsobilý vykonávať dohodnutý druh práce a či v prípade, ak túto prácu bude vykonávať, nebude ohrozený jeho život a zdravie.** Skúmanie zdravotného stavu uchádzača o zamestnanie je pre oblasť pracovnoprávných vzťahov dôležité, hoci ide o veľmi citlivú oblasť a takéto skúmanie zasahuje do telesnej integrity fyzickej osoby a predstavuje súčasť jej osobných údajov. Informácie o zdravotnom stave je oprávnený spracúvať výlučne ten, koho na to oprávňujú osobitné zákony (napr. zákon o zdravotnej starostlivosti). Zamestnávateľ na účel výberu vhodného uchádzača môže spracúvať výlučne informáciu, **či je uchádzač spôsobilý/nespoľsobilý vykonávať prácu na určenej pracovnej pozícii.**

Charakter a obsah lekárskeho vyšetrenia uchádzača o zamestnanie i zamestnanca určuje v nadväznosti na povinnosti zamestnávateľa stanovené v § 30 ods. 1 písm. b) a c) zákona o ochrane, podpore a rozvoji verejného zdravia (povinnosť zamestnávateľa zabezpečiť pre svojich zamestnancov zdravotný dohľad a posudzovanie zdravotnej spôsobilosti na prácu) Vestník Ministerstva zdravotníctva SR čiastka 1-10 z 29. januára 2014. Vestník MZ SR určuje predovšetkým druh a okamih uskutočňovania lekárskeho preventívneho prehliadky s väzbou na faktory práce a pracovného prostredia, resp. práce, pri ktorých zdravotnú spôsobilosť vyžadujú osobitné právne predpisy. **Lekárske preventívne prehliadky na účely posúdenia zdravotnej spôsobilosti pred uzatvorením pracovnoprávneho vzťahu** alebo obdobného pracovného vzťahu fyzickej osoby, ktorá sa uchádza o zamestnanie, sú zamerané na zisťovanie už rozvinutých chorobných náleзов, ale aj klinicky sa neprejavujúcich, ale už zistiteľných rizikových ukazovateľov vzniku choroby z povolania, alebo ochorenia v súvislosti s prácou, ako aj choroby, ktorá by mohla znamenať neskôr vznik zdravotnej kontraindikácie pre vykonávanie danej práce. **Lekárske preventívne prehliadky vo vzťahu k práci** sa vykonávajú u osôb, ktorých práca je zaradená do tretej alebo štvrtej kategórie; u osôb, ktorých práca je zaradená do prvej alebo druhej kategórie sa lekárske preventívne prehliadky vo vzťahu k práci vykonávajú, ak to vyžaduje osobitný predpis, alebo ak o vykonanie lekárskej preventívnej prehliadky zamestnanec požiada. **Periodická lekárska preventívna prehliadka** v súvislosti s výkonom práce sa vykonáva jedenkrát za dva roky u práce zaradenej do tretej kategórie a jedenkrát za rok u práce zaradenej do štvrtej kategórie. Periodická lekárska preventívna prehliadka u osôb vykonávajúcich prácu zaradenú do prvej alebo druhej kategórie, ak to vyžaduje osobitný predpis, sa vykonáva v intervaloch podľa tohto predpisu. Lekárska preventívna prehliadka pred zmenou pracovného zaradenia sa musí vykonať vždy pred realizovaním samotnej zmeny pracovného zaradenia.

Vyšetrenia v rámci lekárskej preventívnej prehliadky vo vzťahu k práci sa delia na **tzv. základné vyšetrenia**, ktoré sa vykonávajú ako neoddeliteľná súčasť každej lekárskej preventívnej prehliadky vo vzťahu k práci v rozsahu ustanovenom pri jednotlivých faktoroch, pri skupinách faktorov alebo vykonávanej práci (sú obsiahnuté v č. 2 až 6 Vestníka MZ SR), a tzv. **doplňkové vyšetrenia**, ktoré sa vykonávajú v odôvodnených prípadoch (sú obsiahnuté v č. 2 až 6 Vestníka MZ SR), sú individuálne indikované lekárom vykonávajúcim lekársku preventívnu prehliadku vo vzťahu k práci; vyplývajú z identifikovaných a posúdených zdravotných rizík, pôsobenia faktorov práce a pracovného prostredia, vykonávanej práce, možného poškodenia zdravia z práce, alebo sú potrebné na vylúčenie kontraindikácií.

Lekárske preventívne prehliadky vo vzťahu k práci, ktoré sú súčasťou zdravotného dohľadu v oblasti ochrany zdravia pri práci, vykonávajú lekári pracovnej zdravotnej služby s príslušnou špecializáciou a lekári so špecializáciou v špecializačnom odbore všeobecné lekárstvo alebo všeobecná starostlivosť o deti a dorast, ktorí nie sú lekármi pracovnej zdravotnej služby.

S ohľadom na ochranu osobných údajov, v kontexte posudzovania psychologickéj spôsobilosti uchádzača o zamestnanie, treba skúmať, či v konkrétnom prípade je po-

vinnosť zamestnanca uložená zamestnávateľom súčasťou výpočtu základného alebo doplnkového **vyšetrenia** v rámci lekárskej preventívnej prehliadky **vo vzťahu k práci, vo väzbe na faktor práce a pracovného prostredia alebo druh práce zamestnanca**, t. j. či zamestnanec má vôbec podstúpiť takéto vyšetrenie (napr. posúdenie psychologickéj spôsobilosti na výkon práce) vo vzťahu k druhu svojej práce. Pokiaľ obsahuje Vestník MZ SR ako súčasť lekárskeho vyšetrenia napr. pri konkrétnom druhu práce psychologické vyšetrenie, ako súčasť základného alebo doplnkového vyšetrenia na posúdenie zdravotnej spôsobilosti, je povinnosťou zamestnanca alebo uchádzača o zamestnanie takéto vyšetrenie podstúpiť, keďže právnym základom spracúvania osobných údajov je v tomto prípade osobitný zákon (zákona o ochrane, podpore a rozvoji verejného zdravia v nadväznosti na Vestník MZ SR). V prípade psychologického vyšetrenia, ako súčasť len doplnkových vyšetrení, treba následne skúmať dôvody nariadenia takéhoto vyšetrenia zo strany lekára, ktorý vykonáva lekársku preventívnu prehliadku vo vzťahu k práci s ohľadom na uvádzané vecné dôvody realizácie doplnkových vyšetrení. Psychologické vyšetrenia, ako súčasť posudzovania zdravotného stavu zamestnancov alebo uchádzačov o zamestnanie, sú dané napr. pri prácach spojených s vedením motorových vozidiel ako súčasť základného vyšetrenia, pri obsluhu kotla I. až V. triedy ako súčasť doplnkového vyšetrenia, pri obsluhu motorových vozíkov ako súčasť doplnkového vyšetrenia a pod.

Za predpokladu, že niektorý z uvedených procesných krokov realizácie psychologického vyšetrenia zamestnanca, ako súčasť posudzovania jeho zdravotnej spôsobilosti na výkon práce, nebol naplnený, nemožno odôvodniť podstúpenie psychologického vyšetrenia požiadavkou osobitného právneho predpisu a takýto prípadný postup zamestnávateľa by bol v priamom rozpore s pracovnoprávnymi predpismi. Obdobne je tento postup rozporný so zákonom o ochrane osobných údajov, keďže v tomto prípade zamestnávateľ môže osobné údaje získať výlučne v rozsahu a spôsobom upraveným osobitným predpisom.

V aplikačnej praxi prichádza k problémom posúdenia zdravotného stavu v prípade, keď ide o zamestnancov, posúdenie zdravotného stavu ktorých je mimo rámca vyššie uvedeného zákona, a teda práve táto skutočnosť je podobná problému zisťovania psychickej spôsobilosti zamestnanca. Zamestnávateľ nesmie na výkon práce zaraďovať zamestnanca, ktorý nie je zdravotne spôsobilý vykonávať takúto prácu. Obdobný zákaz sa uplatňuje aj v predzmluvných vzťahoch v zmysle § 41 ods. 2 ZP, keď zamestnávateľ môže uzatvoriť pracovnú zmluvu s fyzickou osobou zdravotne spôsobilou alebo psychicky spôsobilou na túto prácu, ak túto spôsobilosť vyžaduje osobitný predpis. Podľa § 6 ods. 1 písm. o) zákona o bezpečnosti a ochrane zdravia pri práci je zamestnávateľ, okrem iného, povinný zaraďovať zamestnancov na výkon práce so zreteľom na ich zdravotný stav a nedovoliť, aby vykonávali práce, ktoré nezodpovedajú ich zdravotnému stavu.

V súčasnosti niektorí zamestnávatelia požadujú v rámci výberových konaní rôzne psychologické testovania či vyšetrenia. Vzniká otázka, či zamestnávateľ môže požadovať absolvovať psychologické testovanie či vyšetrenie, ak to nestanovujú osobitné právne

predpisy. Za predpokladu, že ukladanie povinností zamestnancom musí byť v rámci a na základe zákona a ustanovenia Zákonníka práce obsahujúce povinnosti zamestnanca, budeme považovať za kogentné, od ktorých sa nemožno odchýliť, možno usudzovať, že zamestnávateľ **takéto oprávnenia nemá**. Zamestnávateľ je pri ukladaní povinností súčasne viazaný aj druhom a miestom výkonu práce zamestnanca, prípadne dohodnutými pracovnými podmienkami.

V tejto súvislosti by bolo potrebné rozlišovať, či predmetom psychologického vyšetrenia je prostredníctvom psychodiagnostických metód zistiť rysy osobnosti zamestnanca, t. j. jeho výkonové, temperamentové, motivačné a charakterové vlastnosti, ktoré sú potrebné a relevantné na výkon jeho práce, alebo skúmanie jadra osobnosti, ktoré je možné len vtedy, ak to požadujú osobitné právne predpisy (skúmaniu jadra osobnosti nebudeme venovať pozornosť). Je otázne, či zamestnávateľ môže skúmať vyššie uvedené vlastnosti. Pri neexistencii špecifickej úpravy nie je možné jednoducho vychádzať zo základného princípu súkromného práva „je dovolené všetko, čo nie je zakázané“ a možnosť psychologického vyšetrovania dovoliť bez akýchkoľvek mantinelov. Naopak, je nutné použiť princíp, že **ukladanie povinností zamestnancom musí byť na základe zákona, v jeho medziach a pri zachovaní základných práv a slobôd**. Inak povedané, ustanovenia Zákonníka práce obsahujúce povinnosti zamestnanca možno považovať za kogentné, od ktorých sa nemožno odchýliť.

Pri skúmaní problému, či stanoviť právo zamestnávateľa požadovať určitú psychickú spôsobilosť zamestnancov a ich psychologické vyšetrenie možno vychádzať z toho, že Zákonník práce umožňuje, aby si zamestnávateľia, v súlade s konkrétnymi podmienkami ich činnosti, určili pre zamestnancov **požiadavky na riadny výkon práce**. Z dôvodu zachovania právnej istoty Zákonník práce požaduje, aby boli požiadavky na riadny výkon práce stanovené vo vnútornom predpise zamestnávateľa alebo v pracovnej zmluve. Zamestnávateľova možnosť stanoviť požiadavky na výkon práce nie je však neobmedzená. Zamestnávateľ musí postupovať v súlade so **zásadou primeranosti** a požiadavky by mal stanoviť tak, aby boli **pre konkrétnu prácu odôvodniteľné a oprávnené**. Takisto musí platiť, že iba pri splnení požiadavky bude zamestnanec schopný riadneho výkonu svojej práce. V tejto súvislosti je treba zdôrazniť, že je otázne, či je možné, aby si zamestnávateľ stanovil ako požiadavku na výkon práce určitú psychickú spôsobilosť, pretože takéto zisťovanie zasahuje do osobnej integrity zamestnanca a súčasne zasahuje do právneho režimu ochrany osobných údajov, keďže informácie získané z takéhoto zdravotného posúdenia majú charakter osobných údajov. Možno sa preto domnievať, že pre určité druhy prác by malo byť možné požadovať špeciálne schopnosti, vrátane požiadavky na psychickú spôsobilosť, za predpokladu, že skutočne táto **špeciálna spôsobilosť je potrebná a súvisí s konkrétnym druhom práce a s činnosťou vykonávanou v jeho rámci**.

Pokiaľ je vzhľadom na konkrétny druh práce oprávnené, aby si zamestnávateľ stanovil požiadavku psychickej spôsobilosti, domnievame sa, že je aj možné, aby **zamestnávateľ požadoval preukázanie tejto psychickej spôsobilosti** a aby bol zamestnanec

povinný preukázať svoju psychickú spôsobilosť. Toto konštatovanie vychádza z toho, že zisťovanie psychickej spôsobilosti zamestnanca na výkon určitého druhu práce smeruje k tomu, aby zamestnávateľ mal preukázané, či zamestnanec je skutočne spôsobilý vykonávať dohodnutý druh práce.

Zamestnávateľ by mal posudzovať každý prípad osobitne aj pri určovaní povinnosti zamestnanca podrobiť sa psychologickému vyšetreniu. Z tohto dôvodu **plošné nariadenie psychologických vyšetrení všetkých zamestnancov bez rozdielu**, t. j. bez zohľadnenia druhov práce a konkrétnych úloh, ktoré zamestnanci vykonávajú, možno považovať za **neprimerané a neodôvodnené** a v rozpore ako so Zákonníkom práce, tak i zákonom o ochrane osobných údajov (rozširovanie rozsahu spracúvaných osobných údajov rozhodnutím zamestnávateľa bez právneho základu v osobitnom zákone). Na základe judikatúry Najvyššieho súdu ČR⁸¹ by navyše malo byť podstúpenie vyšetrení odôvodnené aj **zistením zamestnávateľa, že zamestnanec má problémy s riadnym výkonom práce**. V súvislosti so zisťovaním spôsobilosti zamestnanca a jeho psychickej spôsobilosti je otázne, či je vôbec možné, aby si zamestnávateľ stanovil, ako požiadavku na výkon práce, určitú psychickú spôsobilosť, pretože takéto zisťovanie zasahuje do osobnej integrity zamestnanca, a preto by bolo potrebné skúmať každý konkrétny prípad – druh práce, pre ktorý by požadovanie určitého druhu psychickej spôsobilosti bolo odôvodnené, primerané a splňalo legitímny účel. Pre určité druhy prác by tak bolo možné požadovať špeciálne schopnosti, napr. verbálne, matematické, mechanické schopnosti; výkonnosť; koncentrácia a pod., ako požiadavku na výkon práce za predpokladu, že skutočne táto **špeciálna schopnosť je potrebná a súvisí s konkrétnym druhom práce a činnosťou vykonávanou v jeho rámci**.

Za požiadavky na riadny výkon práce sa aj na účely realizácie výberového konania, na základe poznatkov aplikačnej praxe a relevantnej judikatúry, považuje najmä požiadavka určitého štýlu obliekania sa, vhodného spoločenského vystupovania (napr. aj mimo pracovného času, ak to vyžaduje povaha práce a charakter zamestnávateľského subjektu, napr. slušné vystupovanie zamestnanca, ktorý je v pozícii vysoko postaveného zamestnanca a de facto reprezentuje zamestnávateľa aj mimo pracovného času), organizačné a riadiace schopnosti, aby si zamestnanec vedel udržať autoritu, aby mal manuálne zručnosti, určité odborné vedomosti, morálne kvality zamestnanca a pod. V aplikačnej praxi by mohlo ísť napr. o prácu zamestnanca, ktorý pracuje v banke s veľkým objemom peňazí a v súvislosti s jeho prácou môže byť ohrozený jeho život (napr. v prípade ozbrojeného prepadnutia banky) a je preto potrebné, aby bol spôsobilý zvládať takéto stresové, hraničné situácie. Ak by sa zamestnanec zúčastnil psychologického vyšetrenia a zamestnávateľ by mal preukázané, že zamestnanec nespĺňa požiadavky dané na výkon jeho práce, prípadne ak by sa zamestnanec za splnenia vyššie uvedených podmienok psychologického vyšetrenia odmietol zúčastniť, dalo by sa uvažovať o tom, že by vznikol výpovedný dôvod podľa § 63 ods. 1 ZP a zamestnávateľ by mohol **skončiť**

81 Rozhodnutie Najvyššieho súdu ČR, sp. zn. 21 Cdo 2627/2007.

pracovný pomer so zamestnancom. Takáto možnosť skončenia pracovného pomeru však musí byť preskúmaná individuálne, pretože hrozí jej neplatnosť.⁸²

Vzhľadom na neexistenciu výslovnej právnej úpravy zisťovania psychickej spôsobilosti zamestnancov si musíme uvedomiť, že posudzovanie právneho základu uskutočnenia psychologického vyšetrenia sa musí uskutočniť v dvoch samostatných právnych režimoch. Zákonník práce, na jednej strane, umožňuje zamestnávateľovi, aby posúdenie psychickej spôsobilosti ustanovil ako požiadavku predchádzajúcu výkonu práce zamestnancov a v nadväznosti na zabezpečenie právnej istoty **získal súhlas všetkých zamestnancov so zisťovaním ich psychickej spôsobilosti** prostredníctvom psychologického vyšetrovania. V prípade, ak súhlas zamestnanca so psychologickým vyšetrením nemá zamestnávateľ k dispozícii, jeho **oprávnenie jednostranne uložiť zamestnancom povinnosť absolvovať psychologické vyšetrenie** je spojené so závažnými rizikami posúdenia jeho konania ako rozporného s právnym poriadkom. Na druhej strane, z hľadiska právneho režimu zákona o ochrane osobných údajov, síce môže zamestnávateľ spracúvať osobné údaje v rozsahu podľa osobitných právnych predpisov a vo výnimočných situáciách ich získavanie spojiť so súhlasom zamestnancov, v uvedenom prípade však psychologické posúdenie spôsobilosti predstavuje taký vážny zásah do základných ľudských práv a slobôd zamestnanca (najmä právo na súkromný a rodinný život), že by nemalo byť, a ani nie je viazané na jeho súhlas s uskutočnením psychického posúdenia spôsobilosti. Z hľadiska právneho režimu zákona o ochrane osobných údajov preto, ak nemožno vykonanie psychického posúdenia zamestnanca odvodiť zo žiadneho osobitného zákona ako právneho základu, nemôže takéto psychologické vyšetrenie zamestnanca zamestnávateľ vykonať. V tomto ohľade musíme opätovne poukázať na problematiku získavania takého súhlasu zamestnanca a potrebu jeho slobodného poskytnutia.⁸³

Vo všeobecnosti, s poukázaním na nedostatočnú právnu úpravu, nie je možné jednoznačne postihnúť všetky riziká psychologického vyšetrovania zamestnancov. V prípade kontroly inšpektorátu práce, ktorý by posúdil, že psychologické vyšetrenia nie sú v súlade a v medziach zákona, hrozila by zamestnávateľovi sankcia – pokuta až do výšky 100 000 € (prípadne by mohol inšpektorát práce uložiť nápravu tohto stavu). Ďalej by v prípade, ak by požiadavka psychickej spôsobilosti bola neodôvodnená a neprimerane zasahovala dôstojnosť zamestnanca, mohlo dôjsť aj k diskriminačnému konaniu zamestnávateľa a zamestnanec by sa mohol domáhať súdnou cestou nápravy tohto stavu (ak by bola vážne poškodená jeho dôstojnosť, aj náhrady nemajetkovej ujmy v peniahoch).

82 Rozhodnutie Najvyššieho súdu ČR, sp. zn. 21 Cdo 628/2006.

83 Podmienky získavania slobodného súhlasu zamestnanca sú bližšie konkretizované v podkapitole 2.3.2.

4.5 Uvádzanie rodného čísla v pracovnej zmluve

Z hľadiska platnosti každého právneho úkonu je nevyhnutné označenie zmluvných strán a ich náležitá identifikácia. Kým absencia označenia zmluvných strán zapríčiní absolútnu neplatnosť právneho úkonu, neúplná či chybná identifikácia automaticky takýto právny účinok nemá. Nepresnosti v označení účastníka zmluvy nespôsobujú neplatnosť zmluvy, ak je nepochybné, kto zmluvu uzavrel.⁸⁴

Žiadne ustanovenia Zákonníka práce výslovne nepredpisujú povinné identifikátory zmluvnej strany. Zamestnávateľ sa tak zvyčajne identifikuje rovnako ako vo svojich obchodných dokumentoch.⁸⁵ Uvádzanie obchodného mena je pritom samozrejmosťou, ale nie povinnosťou, pokiaľ je nepochybné, kto je účastníkom právneho úkonu, ak navyše pracovnoprávne predpisy neobsahujú povinnosť označiť zamestnávateľský subjekt jeho obchodným menom.⁸⁶ Identifikátory požadované od zamestnanca majú v praxi skutočne široký diapazón. Na internetových stránkach možno dohľadať rôzne „zaručene použiteľné“ vzory pracovnej zmluvy alebo niektorej dohody o práci vykonávanej mimo pracovného pomeru, ktoré vyžadujú vyplniť na identifikáciu zmluvnej strany súčasne, ale aj v rôznych kombináciách: meno a priezvisko zamestnanca, rodné priezvisko, dátum a miesto narodenia, rodné číslo, číslo občianskeho preukazu/pasu/iného identifikačného dokladu, adresu bydliska, emailovú adresu, telefónne číslo, rodinný stav a pod. Skôr, ako sa zamestnávateľ rozhodne pre editovanie niektorého vzoru, mal by kvalifikovane posúdiť, ktoré údaje zamestnanca môže z pohľadu práva osobných údajov pre identifikáciu zmluvnej strany spracúvať. Je nevyhnutné rešpektovať predovšetkým účel spracúvania a zoznam, resp. rozsah spracúvaných osobných údajov na daný účel. Súhlas dotknutej osoby so spracúvaním jej identifikačných údajov na účel uzavretia konkrétnej zmluvy sa nevyžaduje, pretože spracúvanie sa uskutočňuje na právnom základe predvídanom v čl. 6 ods. 1 písm. b) GDPR a ust. § 13 ods. 1 písm. b) nového zákona o ochrane osobných údajov.⁸⁷

Rodné číslo je osobným údajom, pretože umožňuje identifikovať konkrétnu fyzickú osobu. V podmienkach Slovenskej republiky⁸⁸ je to jedinečný a trvalý identifikátor

84 Uvedené platí pre akýkoľvek právny úkon. Z rozsudku Najvyššieho súdu Slovenskej republiky sp. zn. 1 Obdo V 2/2006-399 z 30. apríla 2008.

85 V súlade s § 3a zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov je každý podnikateľ povinný na svojich obchodných listoch a objednávkach vyhotovených v písomnej alebo elektronickej forme (ďalej len „obchodné dokumenty“) uvádzať obchodné meno, sídlo alebo miesto podnikania, právnu formu právnickej osoby a identifikačné číslo, ak je pridelené. Podnikatelia zapísaní v obchodnom registri alebo v inej evidencii podnikateľov uvádzajú aj označenie registra, ktorý podnikateľa zapísal, a číslo zápisu.

86 Z nálezku Ústavného súdu Českej republiky IV. ÚS 160/99 z 11. júla 2001, v ktorom sa riešila situácia posúdenia platnosti dohody o hmotnej zodpovednosti. Tá bola súčasťou pracovnej zmluvy, v ktorej sa ale zamestnávateľ označil už neexistujúcim obchodným menom.

87 Ust. § 13 ods. 1 písm. b) nového zákona o ochrane osobných údajov: „Spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov: ... spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby.“

88 Rodné číslo, ako všeobecný identifikátor osôb, požívajú aj v Českej republike.

fyzickej osoby, z ktorého je možné určiť aj ďalšie osobné údaje, a to dátum narodenia (vek) a pohlavie.

Starý zákon o ochrane osobných údajov spomína všeobecne použiteľný identifikátor (rodné číslo) v ust. § 13 ods. 2 v súvislosti s obmedzením jeho použitia len na dosiahnutie daného účelu spracúvania. Ustanovenie § 13 je uvádzané nadpisom „*Osobitné kategórie osobných údajov*“. Na základe danej systematiky Úrad pre ochranu osobných údajov Slovenskej republiky považuje rodné číslo za citlivý údaj.⁸⁹ Podľa zavádzanej koncepcie GDPR a nového zákona o ochrane osobných údajov, už rodné číslo nie je citlivým osobným údajom.

Rodné číslo priamo neodhaľuje žiadnu z citlivých charakteristík fyzickej osoby. Vek a pohlavie patria do kategórie bežných osobných údajov. Nepriamo, vzhľadom na to, že sa rodné číslo využíva na identifikáciu poistencov zdravotného poistenia, môže odhaľovať genetické údaje a údaje týkajúce sa zdravia. Myslíme si, že *pri zohľadnení všetkých prostriedkov, u ktorých je primeraná pravdepodobnosť, že ich osoba využije*, tu existuje skôr hypotetická alebo zanedbateľná možnosť na odhalenie zdravotného stavu konkrétnej fyzickej osoby prostredníctvom jej rodného čísla.⁹⁰ A aj keby rodné číslo pri vynaložení všetkého úsilia odhalilo údaj o zdraví, a tento by ďalej nebol spolu s rodným číslom spracúvaný, nemožno rodné číslo v takomto prípade stále vyhodnotiť ako citlivý údaj. Rodné číslo, v zmysle novej právnej úpravy ochrany osobných údajov, teda nemožno považovať za citlivý údaj a nepodlieha zákazu spracúvania podľa čl. 9 GDPR a ust. § 16 nového zákona o ochrane osobných údajov. Na druhej strane to ale neznamena, že rodné číslo je bežný osobný údaj, ktorý dotknutá osoba musí uvádzať na počkanie každému, kto oň požiada.⁹¹ Spracúvanie rodného čísla má svoje vlastné špecifické pravidlá, možno povedať pravidlá obdobné režimu spracúvania citlivých údajov chrániace socioekonomický status jednotlivca, ktorý by bolo možné inak ľahko odhaliť lustrovaním viacerých databáz verejnej správy.⁹²

Podľa § 78 ods. 4 nového zákona o ochrane osobných údajov *všeobecne použiteľný identifikátor*⁹³ *ustanovený osobitným predpisom* (t. j. zákonom č. 301/1995 Z. z. o rodnom čísle v znení neskorších predpisov) *možno využiť na účely identifikovania fyzickej*

89 Uvedené zodpovedá tiež článku 8 ods. 7 smernice č. 95/46/ES, ktorú GDPR ruší.

90 Pozri k tomu tiež: Stanovisko č. 4/2007 k pojmu osobné údaje vydané Pracovnou skupinou pre ochranu údajov zriadenou podľa článku 29, WP 136.

91 Napríklad do knihy návštev pri vstupe do úradov.

92 Rodné číslo je dovolené právnickými predpismi používať vo sfére zdravotnej starostlivosti (zdravotné poisťovne, nemocnice), štátnej správy školstva, polície, matrik, sociálneho zabezpečenia i daní. Pozri aj: BARANCOVÁ, H. Nové technológie v pracovnom práve a ochrana zamestnanca (možnosti a riziká). Praha: Leges, 2016, s. 25 a nasl.

93 Zákon o ochrane osobných údajov používa na označenie pojmu rodné číslo slovné spojenie všeobecne použiteľný identifikátor, čo umožňuje do budúcnosti reagovať na prípadný prechod od rodného čísla k inému identifikátoru bez potreby legislatívnej úpravy tohto ustanovenia. K bližšej diskusii pozri: KOVÁČ, P. Zrušenie rodného čísla – drahá a zbytočná sranda. Dostupné na internete: <https://dennikn.sk/blog/zrusenie-rodneho-cisla-draha-a-zbytocna-sranda/>. [online]. [cit. 15.09.2017]; alebo aj: ZIMEN, O. Autentifikácia rodným číslom – áno alebo nie? Dostupné na internete: <https://www.pravnenoviny.sk/spravne-pravo/autentifikacia-rodnym-cislom-ano-alebo-nie>. [online]. [cit. 15.09.2017].

osoby len vtedy, ak jeho využitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Kľúčovým je vymedzenie konkrétneho a legitímneho účelu (zámeru) spracúvania rodného čísla na pracovnej zmluve/niektorej z dohôd o práci vykonávanej mimo pracovného pomeru (ďalej len dohoda v príslušnom gramatickom tvare) a posúdenie nevyhnutnosti spracúvania rodného čísla na takto stanovený účel.

Osobné údaje zmluvnej strany uvádzame v pracovnej zmluve/dohode na účely jej identifikovania, ktorým sledujeme založenie a vznik pracovného pomeru. Súhlasíme, že v súlade so zásadou obmedzenia účelu (čl. 5 písm. b) GDPR a § 7 nového zákona o ochrane osobných údajov) a zásadou minimalizácie údajov (čl. 5 písm. c) GDPR a § 8 nového zákona o ochrane osobných údajov) zamestnávateľovi na identifikáciu zamestnanca, ako zmluvnej strany, v plnej miere postačuje uvedenie jeho mena, priezviska, adresy bydliska a roku narodenia. K založeniu a vzniku pracovnoprávneho vzťahu zamestnávateľ nepotrebuje identifikovať druhú zmluvnú stranu jej rodným číslom. Ak zamestnávateľ chce uvádzať rodné číslo v pracovných zmluvách, potrebuje nájsť iný legitímny účel spracúvania rodného čísla.

Po uzavretí pracovnej zmluvy/dohody túto ďalej zamestnávateľ eviduje a uchováva na účely uplatňovania práv a povinností plynúcich z pracovného pomeru. Mimo iného je podľa zákona č. 595/2003 Z. z. o dani z príjmu v znení neskorších predpisov povinný viesť mzdový list zamestnanca, ktorý okrem ďalších údajov obsahuje aj jeho rodné číslo; podľa zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov je povinný prihlásiť zamestnanca na sociálne poistenie identifikačným číslom sociálneho poistenia, ktorým je opäť jeho rodné číslo; rodným číslom sa identifikuje zamestnanec aj v príslušnej zdravotnej poisťovni podľa zákona č. 580/2004 Z. z. o zdravotnom poistení v znení neskorších predpisov a pod. Uvedenie rodného čísla v pracovnej zmluve/dohode je tak prostriedkom k jeho získaniu a sledovaným účelom je „správa“ pracovnoprávneho vzťahu kvôli poistným odvodom, prídavkom, daňovým preddavkom i daňovému bonusu. Sme toho názoru, že získanie rodného čísla jeho uvedením v pracovnej zmluve/dohode a ďalšie spracovateľské operácie s týmto osobným údajom je možné obhájiť práve legitímnym zámerom prevádzkovateľa, keď pracovnú zmluvu/dohodu využíva ako jeden z prostriedkov zhromažďovania rodných čísel pre ich následné využívanie za účelom stanoveným zákonom. Navrhujeme však rešpektovanie niekoľkých pravidiel:

- neodporúčame rodné číslo zamestnanca uvádzať medzi identifikačnými údajmi zmluvnej strany v hlavičke pracovnej zmluvy/dohody z dôvodu odlišenia účelov spracúvania tam uvedených osobných údajov;
- vhodné je do pracovnej zmluvy/dohody zapracovať samostatný článok s miestom pre vyplnenie rodného čísla zamestnanca (napríklad ako v prípade požadovania čísla účtu, na ktorý má byť vyplatená mzda);
- zamestnávateľ by mal stručne informovať dotknutú osobu o účele spracúvania rodného čísla a právnom základe spracúvania, alebo aspoň odkázať na vnútro podnikové pravidlá upravujúce zásady spracúvania a ochrany osobných údajov, v ktorých zamestnanec nájde údaje, o ktorých ho zamestnávateľ musí informo-

- vat⁹⁴; a
- odporúčame formuláciu upozornenia, že pokiaľ zamestnanec nesúhlasí s uvedením rodného čísla v pracovnej zmluve, má povinnosť zamestnávateľovi oznámiť rodné číslo pre zákonmi vyžadované účely iným spôsobom, a to najneskôr do začatia výkonu činnosti zamestnanca.⁹⁵

Z hľadiska aplikácie práva osobných údajov platí, že akákoľvek zmluva, vrátane pracovnej zmluvy, má obsahovať len také identifikátory, ktoré skutočne na identifikáciu zmluvných strán potrebuje. Rodné číslo zamestnanca nie je potrebné na jeho identifikáciu ako zmluvnej strany. Bez znalosti rodného čísla zamestnanca ale nemôže zamestnávateľ riadne plniť niektoré povinnosti uložené mu právnymi predpismi, preto považujeme za možné (viď vyššie odporúčané postupy pre zákonnosť takéhoto kroku), aby zamestnávateľ získaval rodné číslo prostredníctvom pracovnej zmluvy. Nie je však vôbec vhodné uvádzať rodné číslo medzi identifikátormi zmluvnej strany, aby to nezbýdalo k záveru, že toto je účelom spracúvania rodného čísla. V súlade s pravidlami ochrany osobných údajov bude vytvorenie samostatného článku/ustanovenia pracovnej zmluvy so žiadosťou o poskytnutie rodného čísla a s obsahovými náležitosťami tzv. informačnej povinnosti prevádzkovateľa podľa ust. § 19 nového zákona o ochrane osobných údajov. Ďalším riešením je samozrejme upustiť od praktiky získavania rodného čísla prostredníctvom pracovnej zmluvy a zvoliť iný spôsob (napr. vyplňanie personálnych dotazníkov, prostredníctvom ktorých možno získať aj ďalšie potrebné osobné údaje zamestnancov).

Je potrebné si ešte uvedomiť, že súhlas zamestnanca so spracúvaním rodného čísla zamestnávateľ nepotrebuje, ak obmedzí používanie tohto osobného údaju len na taký okruh spracovateľských operácií, ktoré si použitie rodného čísla aj v skutočnosti vyžadujú (spravidla plnenie nahlasovacích povinností zamestnávateľa voči Sociálnej poisťovni, príslušnej zdravotnej poisťovni, správcovi dane a pod.).

4.6 Kopírovanie a skenovanie úradných dokladov zamestnancov

S uzatváraním pracovnej zmluvy, alebo niektorej z dohôd o prácach vykonávaných mimo pracovného pomeru, súvisí v praxi bežne vykonávaná spracovateľská operácia v podobe kopírovania alebo skenovania úradných dokladov zamestnanca (občianskeho preukazu, vodičského preukazu, dokladu o vzdelaní, preukazu poistenca verejného zdravotného poistenia, rodného listu dieťaťa zamestnanca, sobášneho listu zamestnanca a pod.). Podľa ust. § 15 ods. 6 starého zákona o ochrane osobných údajov *získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním*

94 Bližšie k plneniu tzv. informačnej povinnosti ust. § 19 a § 20 nového zákona o ochrane osobných údajov.

95 V súlade s § 231 ods. 1 písm. b) bod 1 zákona č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov je zamestnávateľ povinný zamestnanca prihlásiť do registra poistencov sociálneho poistenia jeho rodným číslom najneskôr pred začatím výkonu činnosti zamestnanca.

alebo iným zaznamenávaním úradných dokladov na nosič informácií možno len vtedy, ak s tým dotknutá osoba písomne súhlasí, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby. To neplatí, ak ide o získavanie osobných údajov na účely a v rozsahu údajov podľa odseku 4 ich zaznamenávaním z úradného dokladu automatizovanými prostriedkami spracúvania a o získavanie osobných údajov na účely uzatvorenia pracovnoprávneho alebo obdobného vzťahu. Podľa starého zákona o ochrane osobných údajov bolo kopírovanie a skenovanie dokladov na pracovnoprávne účely výslovne dovoľené bez súhlasu zamestnanca, či bez toho, aby existovala výslovná právna úprava v osobitnom zákone za predpokladu, že takéto kopírovanie/skenovanie bolo nevyhnutné na účely uzatvorenia pracovnoprávneho alebo obdobného vzťahu. Súčasne zamestnávateľ podľa § 6 ods. 2 písm. d) starého zákona o ochrane osobných údajov bol povinný zabezpečiť, aby sa spracúvali len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie, ako aj rešpektovať osobitnú právnu úpravu čl. 11 základných zásad Zákonníka práce, podľa ktorého zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával. Zamestnávateľ tak mohol kopírovať/skenovať také úradné doklady zamestnanca, pri ktorých vedel odôvodniť, že sú nevyhnutné na účely uzatvorenia pracovnoprávneho vzťahu alebo obdobného vzťahu.

GDPR a nový zákon o ochrane osobných údajov sa však výslovne situáciou kopírovania/skenovania úradných dokladov zamestnancov na účely uzatvárania pracovnoprávneho vzťahu alebo obdobného vzťahu nezaoberajú a neuvádzajú osobitný právny základ pre danú spracovateľskú operáciu. Znamená to, že zamestnávatelia musia upriamiť pozornosť na iné právne tituly, na základe ktorých budú chcieť kopírovať/skenovať úradné doklady zamestnancov, či už na účely uzatvárania pracovnoprávných vzťahov alebo širšie na iné pracovnoprávne účely. Odvolať sa na ust. § 15 ods. 6 starého zákona o ochrane osobných údajov už nebude možné.

Aj naďalej bez súhlasu zamestnanca tak bude možné kopírovať/skenovať úradné doklady zamestnanca, ak tak ustanovuje osobitný predpis (čl. 6 ods. 1 písm. c) GDPR a ust. § 13 ods. 1 písm. c) nového zákona o ochrane osobných údajov), alebo na to má zamestnávateľ preukázateľný oprávnený záujem (čl. 6 ods. 1 písm. f) GDPR a ust. § 13 ods. 1 písm. f) nového zákona o ochrane osobných údajov).

Napríklad podľa zákona č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov je na účely preukazovania nároku, zisťovania, preverovania a kontroly správneho postupu preukazovania nároku na zníženie základu dane, na zamestnaneckú prémie a na daňový bonus, na účely ochrany a domáhania sa práv daňovníka, zamestnávateľa a správcu dane zamestnávateľ oprávnený spracúvať osobné údaje dotknutých osôb, pričom na tieto účely je oprávnený aj bez súhlasu dotknutej osoby získavať jej osobné údaje kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania. V praxi sa zaužívalo, že citované usta-

novenie oprávňuje zamestnávateľa skopírovať si rodný list dieťaťa práve na účely preukazovania oprávnenia zamestnanca uplatniť si daňový bonus a sobášny list zamestnanca na účely uplatňovania nezdaniteľnej časti základu dane na manžela/manželku. Ďalej s povinnosťou umožniť kopírovanie, skenovanie alebo iné zaznamenávanie občianskeho preukazu, by mal zamestnanec počítať pri uzatváraní doplnkového dôchodkového sporenia podľa zákona č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Obdobne citovaný článok 11 Zákonníka práce v spojitosti s ust. § 41 ods. 2 umožňuje zamestnávateľovi skopírovať doklady preukazujúce dosiahnuté vzdelanie zamestnanca potrebné na výkon dohodnutej práce, domnievame sa, že pokiaľ by išlo o vodičov z povolania, zákonné by bolo aj vyhotovenie kópie vodičského preukazu.

Pokiaľ ide o právny základ podľa čl. 6 ods. 1 písm. f) GDPR a ust. § 13 ods. 1 písm. f) nového zákona o ochrane osobných údajov, t. j. spracúvanie na základe oprávneného záujmu prevádzkovateľa, uvedené oprávňuje zamestnávateľa vyhotoviť kópie takých dokladov, ktoré je povinný mať k dispozícii napríklad pre prípadnú kontrolu oprávneného štátneho orgánu.

Po účinnosti GDPR a nového zákona o ochrane osobných údajov sa v súvislosti s kopírovaním úradných dokumentov zamestnancov teda menia právne základy pre takúto spracovateľskú operáciu. Je potrebné si však uvedomiť, že spracúvanie osobných údajov je zákonné nielen vtedy, ak sa deje na právnom základe, ale kumulatívne ruka v ruku s rešpektovaním zásad spracúvania osobných údajov. Nová právna úprava ochrany osobných údajov stanovuje síce iné právne základy⁹⁶ pre kopírovanie/skenovanie úradných dokladov zamestnanca, no rovnako, ako tá predchádzajúca, núti zamestnávateľa, aby komplexne prehodnotil, či kopírovanie/skenovanie úradných dokladov je naozaj nevyhnutné, a či takýmto spôsobom nezíska aj osobné údaje, ktoré na zamýšľaný účel vôbec nepotrebuje. Ak preukázanie relevantnej skutočnosti je možné dosiahnuť aj iným prostriedkom, ktorý v menšej miere zasahuje do súkromia zamestnanca, má zamestnávateľ využiť tento iný prostriedok a nekopírovať/neskenovať úradný doklad zamestnanca.

4.7 Vedenie osobného (personálneho) spisu zamestnanca

Vznikom pracovnoprávneho vzťahu sa o zamestnancovi zakladá tzv. osobný (personálny) spis zamestnanca. Dokumentácia obsahuje všetky podstatné skutočnosti vyplývajúce z uplatňovania práv a povinností z existujúceho pracovnoprávneho vzťahu, najmä pracovnú zmluvu alebo niektorú z dohôd o prácach vykonávaných mimo pracovného pomeru, osobný dotazník, doklady a potvrdenia vyžadované zamestnávateľom týkajúce sa vzniku, priebehu a skončenia pracovného pomeru. Súčasťou osobného spisu zamestnanca môžu byť všetky osobné údaje, týkajúce sa nielen zamestnanca, ale aj jeho

⁹⁶ K právnym základom spracúvania všeobecných osobných údajov pozri 2.3.2.1. K právnym základom spracúvania citlivých osobných údajov pozri 2.3.2.2.

rodinných príslušníkov, ak ich osobné údaje sú nevyhnutné pre uplatňovanie práv a povinností (napr. rodný list dieťaťa, potvrdenie o návšteve školy, informácia o uzatvorení manželstva a pod.). Súčasťou osobného spisu zamestnanca môžu byť aj kópie úradných dokladov (bližšie kapitola 4.6.). Osobný spis zamestnanca môže obsahovať aj informácie (osobné údaje) týkajúce sa jeho osobného, súkromného života (napr. čerpanie pracovného voľna pri narodení dieťaťa), ktoré je zamestnanec povinný poskytnúť na dokladovanie nároku na čerpanie pracovného voľna.

„Správa registratúry“ je spravidla samostatný informačný systém osobných údajov, v ktorom zamestnávateľ spracúva (uchováva, zhromažďuje, preskupuje, vyhľadáva a pod.) osobné údaje na účel plnenia povinností podľa zákona č. 395/2002 Z. z. Zamestnávateľia uchovávajú a likvidujú dokumenty (registratúrne záznamy a spisy) obsahujúce aj osobné údaje podľa riadne schváleného registratúrneho plánu, ktorý obsahuje lehoty uchovávania jednotlivých registratúrnych záznamov podľa ich dôležitosti. Pri určovaní lehôt vychádza zamestnávateľ z podmienok spracúvania osobných údajov, lehôt určených osobitnými zákonmi na uchovávanie rôznych registratúrnych záznamov (napr. zákon o účtovníctve) a z podmienok likvidácie osobných údajov po skončení účelu ich spracúvania. V podmienkach každého zamestnávateľa sú spracúvané osobné údaje na účely spracúvania účtovných dokladov podľa osobitných zákonov (napr. zákon o účtovníctve, zákon o dani z pridanej hodnoty, Zákonník práce, zákon o sociálnom fonde, zákon o dani z príjmov). V tomto informačnom systéme osobných údajov spracúva zamestnávateľ osobné údaje spravidla o svojich zamestnancoch, ako aj o zamestnancoch klientov, alebo dodávateľov, alebo o klientoch, ak sú fyzickými osobami. Lehota uchovávania osobných údajov na účtovných dokladoch je určená osobitným zákonom o účtovníctve. Osobný spis zamestnanca, vedený zamestnávateľom, môže mať podľa zákona č. 395/2002 Z. z. archívnu hodnotu a po jeho odovzdaní (v súlade so schváleným registratúrnym plánom) do príslušného archívu je k osobným údajom, v ňom obsiahnutým, obmedzený prístup po dobu 90 rokov od vzniku záznamu. Osobný spis zamestnanca je vhodné uchovávať minimálne po dobu, ako sú uchovávané ročné mzdové listy, t. j. 50 rokov.

Vedenie osobného spisu zamestnanca a spracúvanie osobných údajov v jeho obsahu sa tak spravidla uskutočňuje na právnom základe osobitných zákonov, t. j. bez súhlasu zamestnanca, hoci v niektorých prípadoch a kategóriách osobných údajov sa vyžaduje jeho súhlas (napr. fotografia zamestnanca, pozri ďalej).

4.8 Fotografia zamestnanca a zverejňovanie ďalších osobných údajov zamestnanca

Podľa doteraz presadzovanej koncepcie bola fotografia (ale napríklad aj záznam z kamerového systému) považovaná za citlivý osobný údaj, pretože mohla odhaľovať rasový, etnický pôvod, či údaj týkajúci sa zdravia, pre ktoré platí všeobecný zákaz spracúvania. Fotografia skutočne odhaľuje vysoko citlivé osobné údaje, ale pokiaľ sa tieto nespracúvajú, nie je dôvod fotografiu považovať za citlivý osobný údaj podliehajúci re-

žimu osobitných právnych základov spracúvania (viď kapitola 2.3.2.2.), ale ide o všeobecný osobný údaj. Ako má teda zamestnávateľ postupovať, ak chce nechať zamestnancom vyrobiť vizitky s ich fotografiou, či zverejniť fotografie kľúčových zamestnancov na webovom sídle, pretože to zvyšuje dôveryhodnosť firmy a uľahčuje komunikáciu so zákazníkmi?

Zamýšľaný postup zamestnávateľa je možné zahrnúť pod spracovateľské operácie/spracúvanie ako **sprístupňovanie**, či je **zverejňovanie** osobných údajov. V porovnaní so starým zákonom o ochrane osobných údajov už nie sú tieto pojmy v novej právnej úprave samostatne zadefinované, ale na svojom etymologickom význame samozrejme nestrácajú.⁹⁷ Zamestnávateľ je napríklad povinný v zákonom stanovenom rozsahu podľa zákona o sociálnom poistení *poskytnúť* osobné údaje Sociálnej poisťovni, informácie o platových pomeroch vedúcich zamestnancov je zamestnávateľ povinný *sprístupniť* žiadateľovi podľa zákona o slobode informácií. Zamestnávateľ môže poskytnúť osobné údaje o zamestnancovi aj na základe žiadosti zamestnanca (súhlasu zamestnanca), a to napr. na účely potvrdenia o príjme, ktoré zamestnanec dokladuje pri žiadosti o poskytnutie úveru. V prípade telefonického overovania bonity zamestnanca u zamestnávateľa musí zamestnávateľ disponovať súhlasom zamestnanca, komu a v akom rozsahu môže osobné údaje poskytnúť. Citlivo je potom potrebné pristupovať k *zverejňovaniu* osobných údajov, pretože ide o spracovateľskú operáciu, ktorá je spôsobilá ohroziť súkromie zamestnanca skutočne vo vysokej miere. Osobné údaje sa zverejnením stávajú voľne dostupné a dotknutá osoba stráca nad nimi kontrolu.

Na spracúvanie fotografie zamestnanca ako každého iného osobného údajá potrebuje zamestnanec buď súhlas zamestnanca alebo iný právny základ.

Bez súhlasu zamestnanca možno **poskytnúť** alebo **zverejniť** osobné údaje v rozsahu uvedenom v ust. § 79 ods. 3 nového zákona o ochrane osobných údajov, t. j. *titul, meno, priezvisko, pracovné zaradenie, služobné zaradenia, funkčné zaradenie*, osobné číslo zamestnanca alebo zamestnanecké číslo zamestnanca, odborný útvar, miesto výkonu práce, telefónne číslo, faxové číslo, adresu elektronickej pošty na pracovisko a identifikačné údaje zamestnávateľa. V porovnaní so starým zákonom o ochrane osobných údajov bol taxatívny zoznam osobných údajov zamestnanca, ktoré možno poskytnúť alebo zverejniť rozšírený o osobné číslo zamestnanca, resp. jeho zamestnanecké číslo. Fotografia zamestnanca, aj napriek tomu, že sa v návrhu nového zákona o ochrane osobných údajov pôvodne uvažovalo o jej zaradení medzi údaje vymenované v ust. § 79 ods. 3, bola zo zoznamu vyškrtnutá. V tejto súvislosti je potrebné upozorniť na dve skutočnosti.

⁹⁷ Podľa ust. § 4 ods. 3 písm. a) starého zákona o ochrane osobných údajov sa poskytovaním osobných údajov rozumelo odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva; sprístupňovaním osobných údajov bolo oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva a za zverejňovanie osobných údajov sa považovalo publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v opere, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.

Ad 1) Účel poskytnutia alebo zverejnenia osobných údajov vymenovaných v ust. § 79 ods. 3 nového zákona o ochrane osobných údajov nie je obmedzený. Bez súhlasu zamestnanca možno tieto údaje poskytnúť alebo zverejniť, len ak je to potrebné v súvislosti s plnením jeho pracovných povinností, služobných povinností alebo funkčných povinností. Súvislosť s plnením pracovných, služobných alebo funkčných povinností je potrebné posudzovať vždy vzhľadom na okolnosti konkrétneho prípadu. Ako také možno vyhodnotiť konanie zamestnávateľa, ktorý sa rozhodne vyššie uvedené osobné údaje zamestnancov zverejniť na svojom webovom sídle z dôvodu zjednodušenia a zefektívnenie komunikácie s klientmi. Poskytovanie osobných údajov alebo zverejnenie osobných údajov pritom nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.

Ad 2) Ust. § 79 ods. 3 nového zákona o ochrane osobných údajov je zákonným osobitným právnym základom, ktorý jednoznačne stanovuje, aký zoznam osobných údajov zamestnanca, na aký účel možno poskytnúť alebo zverejniť. Nesprávny je potom postup v praxi, ak sa prevádzkovateľ rozhodne, že na daný účel rozšíri zoznam osobných údajov bez ohľadu na to, že si na takúto spracovateľskú operáciu vyžiada súhlas zamestnanca. Na účel vymedzený osobitným zákonom môže prevádzkovateľ spracúvať len tie osobné údaje bez súhlasu dotknutej osoby, ktoré príslušný osobitný zákon presne vymedzuje. Nemôže na ten istý účel rozšíriť rozsah spracúvaných osobných údajov vlastným rozhodnutím alebo prostredníctvom súhlasu dotknutej osoby. V okamihu, keď osobitný zákon vymedzil účel, okruh dotknutých osôb, zoznam/rozsah spracúvaných osobných údajov, podmienky spracúvania, je nimi prevádzkovateľ striktné viazaný bez možnosti odchylného postupu.⁹⁸ Ak raz ust. § 79 ods. 3 nového zákona o ochrane osobných údajov nedovoľuje poskytnúť alebo zverejniť fotografiu zamestnanca na účely plnenia pracovných, služobných alebo funkčných povinností, nemôže zamestnávateľ „obísť“ toto ustanovenie tak, že vyžiadanim súhlasu zamestnanca so zverejnením fotografie rozšíri zoznam osobných údajov, ktoré možno na účely plnenia pracovných, služobných alebo funkčných povinností poskytovať alebo zverejňovať.

Zamestnávateľ teda môže spracúvať fotografiu zamestnanca:

a) na základe súhlasu zamestnanca;

Pozor však na správne vymedzenie účelu spracúvania. Napríklad fotografia zamestnanca môže byť na základe súhlasu zamestnanca spracúvaná na účely zvýšenia dôveryhodnosti firmy, na účely propagácie spoločnosti, na účely zvýšenia záujmu klientov o služby poskytované spoločnosťou, na účely efektívneho vedenia dochádzky, dokumentovania činnosti prevádzkovateľa (firemné akcie) a pod. Súhlas zamestnanca bude zamestnávateľ potrebovať aj vtedy, ak chce napríklad na svojom webovom sídle uverejniť fotografie z rôznych teambuildingových akcií.

98 ŠVEC, M., VALENTOVÁ, T. Ochrana osobných údajov v pracovnoprávných vzťahoch. Bratislava: Wolters Kluwer, 2016, s. 38.

- b) na základe osobitného zákona;

Zamestnávateľ nepotrebuje súhlas zamestnanca na spracúvanie jeho fotografie, ak ho na to oprávňuje osobitný právny predpis, napr. zákon č. 473/2005 Z. z. o poskytovaní služieb v oblasti súkromnej bezpečnosti a o zmene a doplnení niektorých zákonov (zákon o súkromnej bezpečnosti), ktorý upravuje povinnosť vydať identifikačný preukaz obsahujúci aj fotografiu držiteľa takéhoto preukazu. Rovnako tiež zákon č. 55/2017 Z. z. o štátnej službe v znení neskorších predpisov, ktorý predpisuje služobnému úradu povinnosť vydať služobný preukaz štátneho zamestnanca a ktorý okrem iných osobných údajov obsahuje aj fotografiu štátneho zamestnanca. V prípade, že zamestnávateľ spracúva osobné údaje zamestnanca na základe osobitného zákona, možno tieto údaje z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne tretie strany, ktorým sa osobné údaje poskytnú (§ 13 ods. 2 nového zákona o ochrane osobných údajov).

- c) na základe oprávneného záujmu prevádzkovateľa;

Zamestnávateľ môže spracúvať fotografiu zamestnanca bez jeho súhlasu aj vtedy, ak to dokáže zdôvodniť oprávneným záujmom. Pôjde najmä o špecifické situácie, ak z dôvodov zabezpečenia bezpečnosti prevádzky, bude zamestnávateľ takýmto spôsobom regulovať vstup nielen zamestnancov, ale aj rôznych externých subjektov, ktoré pravidelne vstupujú do jeho areálu (fotografia zamestnanca na identifikačnej kartičke).

Polemizovať možno nad situáciou, či by bolo možné spracúvať osobitne fotografiu zamestnanca bez jeho súhlasu na účely evidencie dochádzky, resp. pracovného času (viď aj kapitola 4.8.). Možno záujem zamestnávateľa na tom, aby zamestnanci úmyselne neskresľovali evidenciu svojho pracovného času klasifikovať ako oprávnený záujem? Sme toho názoru, že vedenie evidencie dochádzky zamestnancov s využitím ich fotografie z dôvodu zvýšenia právnej istoty zamestnávateľa nemožno subsumovať pod oprávnený záujem, pretože zamestnávateľ má k dispozícii pre plnenie evidenčnej povinnosti podľa § 99 Zákonníka práce menej invazívne prostriedky zasahujúce do záujmov a práv dotknutej osoby (napr. vrátna služba, identifikácia PIN kódom, RFID kartou, či QR kódom). Nevylučujeme však vedenie evidencie dochádzky vyhotovovaním fotografie zamestnanca na inom právnom základe, konkrétne na základe súhlasu zamestnanca. Zákonník práce na tento účel neupravuje konkrétny druh osobných údajov, ktoré má zamestnávateľ spracúvať, aby bol schopný zaznamenať začiatok a koniec pracovného času, čo znamená, že udelením súhlasu nedôjde k rozšíreniu zákonom dovoleného zoznamu alebo rozsahu osobných údajov, ktoré je možné spracúvať. Evidencia dochádzky vyhotovovaním fotografie zamestnanca vždy pri príchode do zamestnania a po odchode zo zamestnania je možná, ak zamestnanec vyjadrí

súhlas so spracúvaním svojej fotografie na tieto účely. Ak zamestnanec odmietne udeliť súhlas na spracúvanie jeho fotografie na účely evidencie dochádzky, je zamestnávateľ povinný vo vzťahu k tomuto zamestnancovi zabezpečiť evidenciu dochádzky iným spôsobom. Za odmietnutie udeliť súhlas nesmie zamestnávateľ zamestnanca žiadnym spôsobom postihovať, či znevýhodňovať.

4.9 Evidencia dochádzky a vstup do priestorov založený na biometrickom údají

Súčasťou spracúvania osobných údajov o zamestnancoch v pracovnoprávných vzťahoch je aj povinnosť zamestnávateľa viesť evidenciu pracovného času tak, aby bol zaznamenaný začiatok a koniec časového úseku, v ktorom zamestnanec prácu vykonával. Evidencia pracovného času je/môže byť súčasťou informačného systému osobných údajov vedeného na účel personalistiky a miezd. S cieľom zabezpečiť efektívnosť, presnosť a pravdivosť sledovaných údajov zavádzajú zamestnávatelia rôzne elektronické zariadenia, ktoré sú spôsobilé snímať fotografiu, biometrické údaje (odtlačky prstov, odtlačok dlane, biometriu tváre a pod.), alebo fungujú na princípe čipových, alebo bezkontaktných kariet, alebo zadávania prideleného kódu.

Spoločným menovateľom elektronických systémov dochádzky je spracúvanie osobných údajov zamestnancov, ktoré sú spravidla snímané/získavané a často aj uchovávané priamo v zariadení alebo prenášané na úložisko určené klientom (zamestnávateľom). Zariadenie pracuje spolu so softvérom, ktorý umožňuje následné spracovateľské operácie so získanými údajmi. Pre zamestnávateľa je podstatný rozsah/zoznam osobných údajov, ktoré na účel dochádzky spracúva. Zákoník práce nedefinuje zoznam osobných údajov, ktoré je zamestnávateľ oprávnený na účely dochádzky spracúvať. Z hľadiska ochrany osobných údajov môže zamestnávateľ na evidenciu dochádzky podľa Zákoníka práce využiť tie osobné údaje zamestnanca, ktorými disponuje na základe osobitných zákonov a existujúceho pracovnoprávneho vzťahu, a zároveň v rozsahu, ktorý je pre vedenie dochádzky nevyhnutný. Ide o osobné údaje v rozsahu najmä meno a priezvisko zamestnanca, pracovné zaradenie, príchod/odchod zamestnanca, dôvod prerušenia práce (napr. prestávka na odpočinok, pracovná cesta, prekážka v práci a pod.). Požiadavka zamestnávateľa na zvýšenie miery istoty pri evidencii dochádzky je spravidla spojená s pridaním ďalších osobných údajov zamestnanca, ktoré zamestnávateľ nemôže spracúvať bez jeho súhlasu (napr. fotografia zamestnanca - bližšie kapitola 4.8.).

Keďže biometrické údaje zabezpečujú jednoznačnosť a nie nezameniteľnosť jednotlivca a rozmach rôznych technológií priniesol aj ich finančnú dostupnosť, čoraz viac bežných zamestnávateľov rozmyšľa nad inštaláciou a využívaním technológií založených na biometrii na evidenciu dochádzky zamestnancov či na kontrolovaný vstup do určitých priestorov.

Podľa čl. 4 bod 14 GDPR a ust. § 5 písm. c) nového zákona o ochrane osobných údajov biometrickými údajmi sú *osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej*

osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu, alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre, alebo daktyloskopické údaje.

Biometrické údaje sú druhom citlivých osobných údajov, čo znamená, že spracúvanie biometrických údajov sa vo všeobecnosti zakazuje, pokiaľ neexistuje spracovateľská výnimka. Prevádzkovateľ môže spracúvať biometrický údaj, ak má na spracovateľskú operáciu tohto údaju výslovný súhlas⁹⁹ dotknutej osoby, alebo bez jej súhlasu, ak spracúva biometrický údaj na základe niektorého právneho základu uvedeného v čl. 9 ods. 2 GDPR a ust. § 16 ods. 2 nového zákona o ochrane osobných údajov, alebo právneho základu uvedeného v ust. § 79 ods. 5 nového zákona o ochrane osobných údajov. Právna úprava ochrany osobných údajov, účinná od 25. mája 2018, tak evidentne rozširuje právne tituly spracúvania biometrických údajov a možno povedať, že aj uvoľňuje prísnu právnu úpravu spracúvania biometrických údajov, ktorá platila doposiaľ. Spracúvanie biometrických údajov už totiž nepodlieha ani posúdeniu Úradu v konaní o osobitnej registrácii, v ktorej Úrad posudzoval primeranosť ich spracúvania, nevyhnutnosť a právny základ.

No aj napriek tomu, že právne tituly spracúvania biometrických údajov boli rozšírené a povinnosť osobitnej registrácie bola zrušená, nemožno uvedené vykladať tak, že spracúvanie biometrických údajov zamestnancov sa stalo všeobecne prístupnou možnosťou. Stále je potrebné mať na pamäti zásadu, že spracúvanie citlivých údajov sa všeobecne zakazuje (ich spracúvanie je výnimkou) a vyžaduje súčasné aplikovanie ďalších základných zásad spracúvania osobných údajov, predovšetkým zásady obmedzenia účelu a zásady minimalizácie údajov. Ešte skôr, ako prevádzkovateľ formálne pristúpi k skúmaniu toho, či potrebuje súhlas dotknutej osoby na spracúvanie niektorého jej biometrického údaju, alebo sa odvolá na niektorý z iných právnych základov, má kvalifikovane posúdiť, či na účel, ktorý zamýšľa, skutočne a nevyhnutne potrebuje spracúvať takýto druh citlivého údaju. V súlade so zásadou minimalizácie osobných údajov totiž spracúvané osobné údaje musia byť primerané i relevantné vzhľadom na účel, na ktorý sa spracúvajú. Ak sa teda zamestnávateľ rozhodne pre zavedenie evidencie dochádzky alebo obmedzenie vstupov do vyhradených priestorov na základe snímania a uchovávanie niektorého biometrického údaju zamestnanca, mal by zohľadniť nevyhnutnosť zavedenia takéhoto biometrického systému a položiť si základné otázky. Je potenciálne ohrozenie alebo strata súkromia zamestnanca primeraná očakávanému výsledku? Nemožno zamýšľaný účel dosiahnuť iným, menej rušivým prostriedkom?

Zo stanovísk Úradu a správ o stave ochrany osobných údajov vyplýva,¹⁰⁰ že Úrad akceptoval, ak bol biometrický systém využívaný iba na účely kontrolovaného vstupu do objektov, ktorých povaha si vyžaduje špecifické zabezpečenie (napr. jadrové elek-

⁹⁹ K tomu, čo je to výslovný súhlas pozri kapitolu 2.3.2.2.

¹⁰⁰ Správa o stave ochrany osobných údajov za roky 2009 až 2010, tiež správa o stave ochrany osobných údajov za roky 2011 až 2012. Dostupné na: <https://dataprotection.gov.sk/uouu/>.

trárne, muničné sklady, špeciálne laboratóriá, technické zariadenia s vysokou mierou rizika a pod.). Úrad neuznával zavedenie biometrického systému dochádzky, pretože takýto účel (evidencia dochádzky a predchádzanie porušovania pracovnej disciplíny) sa dá z hľadiska primeranosti a nevyhnutnosti rovnako efektívne dosiahnuť aj inými prostriedkami, ktoré sú z pohľadu ochrany osobných údajov dotknutých osôb menej rizikové (napr. vrátna služba alebo elektronický dochádzkový systém a pod.).¹⁰¹ Sme toho názoru, že uvedené platí naďalej.

Zavedenie biometrického systému dochádzky je v rozpore so zásadami spracúvania osobných údajov (zásada obmedzenia účelu a zásada minimalizácie údajov podľa nového zákona o ochrane osobných údajov), pretože zamýšľaný účel je možné dosiahnuť menej invazívnym prostriedkom. Zavedenie biometrického systému na účely evidencie alebo identifikácie vstupu do citlivých, osobitne chránených objektov, vyhradených priestorov alebo prístupu do technických zariadení alebo prístrojov s vysokou mierou rizika je prípustné. Bezproblémové je potom spracúvanie biometrických údajov na základe zákona.¹⁰² No len málo zamestnávateľov sa však môže odvolať na tento druh právneho základu spracúvania biometrických údajov.

Do účinnosti GDPR a nového zákona o ochrane osobných údajov mohli zamestnávatelia oprieť spracúvanie biometrických údajov zamestnanca na účely vstupu do vyhradených priestorov o právny základ uvedený v ust. § 10 ods. 3 písm. g) starého zákona o ochrane osobných údajov, t. j. spracúvanie osobných údajov je nevyhnutné na ochranu práv a právom chránených záujmov prevádzkovateľa (tzv. oprávnený záujem prevádzkovateľa). Od účinnosti GDPR a nového zákona o ochrane osobných údajov nie je oprávnený záujem prevádzkovateľa právnym titulom spracúvania biometrických osobných údajov dotknutej osoby (viď čl. 9 ods. 2 GDPR a ust. § 16 ods. 2 zákona o ochrane osobných údajov). Po lustrácii jedenástich právnych základov pre spracúvanie citlivých osobných údajov sa domnievame, že na spracúvanie biometrického osobného údajá zamestnanca, za účelom jeho vstupov do vyhradených priestorov, bude zamestnávateľ potrebovať súhlas (navyššie **výslovný** súhlas, keďže ide o citlivý údaj) zamestnanca.

Všeobecná uplatniteľnosť súhlasu zamestnanca na spracovateľské operácie s osobnými (nielen biometrickými) údajmi je pritom v pracovnoprávných vzťahoch veľmi

101 V určitých prípadoch v rámci osobitnej registrácie Úrad (na základe rozhodnutia) povolil dochádzkový systém zahŕňajúci biometriu, súčasne však takéto spracúvanie podmienil súhlasom dotknutej osoby. Bližšie: ŠVEC, M., VALENTOVÁ, T. Ochrana osobných údajov v pracovnoprávných vzťahoch. Bratislava: Wolters Kluwer, 2016, s. 52.

102 Ide o osobitný druh právneho základu, ktorý je vyjadrený v ust. § 78 ods. 5 nového zákona o ochrane osobných údajov: Prevádzkovateľ môže spracúvať genetické údaje, biometrické údaje a údaje týkajúce sa zdravia aj na právnom základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná. Pôjde napríklad o zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 647/2007 Z. z. o cestovných dokladoch a o zmene a doplnení niektorých zákonov, zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov, zákon č. 78/2015 Z. z. o kontrole výkonu niektorých rozhodnutí technickými prostriedkami a o zmene a doplnení niektorých zákonov, zákon č. 404/2011 Z. z. o pobyte cudzincov a o zmene a doplnení niektorých zákonov a pod.

vágna, pretože z titulu nerovného postavenia zamestnávateľa a zamestnanca sa prezumuje, že tento súhlas je málokedy skutočne slobodný a neovplyvnený strachom z následkov odmietnutia súhlasu na samotnú existenciu pracovnoprávného vzťahu. A tak, aj keď nová právna úprava rozširuje právne tituly spracúvania citlivých osobných údajov a upúšťa od povinnosti osobitnej registrácie, je pre tých zamestnávateľov, ktorí nenájdu právny základ spracúvania biometrických údajov v osobitnom zákone, prísnejšia v tom smere, že jediným prakticky využiteľným právnym základom z jedenástich právnych základov spracúvania citlivých osobných údajov je len súhlas zamestnanca, pričom zamestnávateľ je povinný uniesť dôkaznú pozíciu, že tento súhlas je výslovný, bol daný slobodne a zamestnávateľ sa musí prakticky vysporiadať so situáciou, keď zamestnanec súhlas odmietne udeliť, či súhlas kedykoľvek odvolá.

4.10 Monitorovanie komunikačných prostriedkov na pracovisku

Pri plnení pracovných povinností využívajú zamestnanci rôzne komunikačné prostriedky, ktoré im zamestnávateľ poskytuje spravidla len na plnenie pracovných povinností (niekedy môže zamestnanec využívať tieto prostriedky aj na súkromné účely v rozsahu a spôsobom dohodnutým so zamestnávateľom). Súčasný technický a technologický pokrok umožňuje veľmi jednoduché a efektívne sledovanie činnosti zamestnanca, počnúc kontrolou webovej aktivity zamestnanca, monitoringom e-mailovej komunikácie, procesov a aplikácií na koncovej stanici, kontrolou zamestnanca prostredníctvom inteligentného snímania obrazovky a klávesnice, zaznamenávaním telefonických hovorov až po využívanie geolokalizačných služieb.¹⁰³ Pri všetkých zmienovaných spôsoboch, využívaných zamestnávateľmi často s cieľom zefektívniť a skvalitniť činnosť spoločnosti, je veľmi náročné vylúčiť spracúvanie osobných údajov. Zamestnávateľ by musel nastaviť také podmienky monitorovania, ktoré by vylúčili možnosť spojiť sledovaný výsledok s konkrétnym zamestnancom. Zamestnávatelia sa často domnievajú, že zavedenie takého monitorovania na iný účel (napr. monitorovanie produktivity práce podľa definovaných kritérií), než je definovaný v § 13 ods. 4 Zákonníka práce, nespadá do pôsobnosti Zákonníka práce, príp. sa domnievajú, že spracúvajú osobné údaje o zamestnancoch na pôvodný účel realizácie pracovnoprávných vzťahov.

Zamestnávateľ pri zavedení rôznych foriem monitorovania spravidla spracúva osobné údaje o zamestnancoch (okrem napr. monitorovania dátových tokov bez možnosti identifikácie jednotlivých pracovných staníc). Je teda povinný definovať účel ich spracúvania, pričom je povinný rešpektovať ustanovenia Zákonníka práce, GDPR, zákona o ochrane osobných údajov a ďalších všeobecne záväzných právnych predpisov. Pri definovaní jasného, zrozumiteľného a zákonného účelu musí zamestnávateľ zohľadniť primeranosť zásahu do práv a právom chránených záujmov zamestnanca (do jeho súkromia) vo vzťahu k sledovanému cieľu (účelu spracúvania osobných údajov), t. j. je

103 Pozri aj: DOLOBÁČ, M. Kontrola elektronických komunikačných prostriedkov v pracovnoprávných vzťahoch. In: Právo, obchod, ekonomika VI.: zborník príspevkov z vedeckej konferencie: 26. - 28. októbra 2016, Vysoké Tatry. - Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016, s. 145-152. ISBN 9788081524431.

vždy potrebné skúmať, či stanovený cieľ (záujem zamestnávateľa) prevažuje nad právom na súkromie, ochranu práv a právom chránených záujmov zamestnanca.

Monitorovanie komunikačných prostriedkov na pracovisku je spravidla vykonávané na základe § 13 ods. 4 Zákonníka práce (zavedenie kontrolného mechanizmu zamestnávateľom) a/alebo na základe § 10 ods. 3 písm. g) starého zákona o ochrane osobných údajov (ochrana práv a právom chránených záujmov prevádzkovateľa/zamestnávateľa). Tieto právne základy sú na monitorovanie komunikačných prostriedkov využiteľné aj po nadobudnutí účinnosti GDPR. GDPR nemá dosah na ust. 13 ods. 4 Zákonníka práce a oprávnený záujem, ktorý sleduje prevádzkovateľ podľa ust. § 10 ods. 3 písm. g) starého zákona o ochrane osobných údajov, má svoj rovnocenný ekvivalent vyjadrený v čl. 6 ods. 1 písm. g) GDPR a ust. § 13 ods. 1 písm. g) nového zákona o ochrane osobných údajov.

Monitorovanie komunikačných prostriedkov u zamestnancov môže zahŕňať monitoring:

- 1) telefonických hovorov;
- 2) webovej aktivity a PC;
- 3) elektronickej pošty;
- 4) polohy zamestnanca.

K 1) Monitorovanie telefonických hovorov

S monitorovaním telefonických hovorov sa stretávame spravidla pri tzv. call centrách, alebo iných službách spojených s komunikáciou zamestnanca s klientom. Zamestnávateľ môže určiť, že cieľom monitorovania bude primárne klient (spravidla na základe jeho súhlasu alebo osobitného zákona). Ak telefonická komunikácia vyplýva zamestnancovi priamo z pracovnej zmluvy, je súčasťou plnenia jeho povinností, nie je potrebné určovať iný účel oddelene pre zamestnanca. Je však nevyhnutné dbať, aby zaznamenané hovory boli využité výlučne na stanovený účel (napr. preukazovanie uzatvorenia zmluvného vzťahu prostredníctvom telefónu), t. j. zamestnávateľ by ich nemal využívať na kontrolu zamestnanca. Pokiaľ chce zamestnávateľ využiť zaznamenané hovory aj na kontrolu plnenia povinností, ktoré zamestnancovi vyplývajú z existujúceho pracovnoprávneho vzťahu, t. j. z pracovnej zmluvy, vnútropodnikových predpisov, pracovného poriadku, musí na tento účel zaviesť kontrolný mechanizmus v zmysle § 13 ods. 4 Zákonníka práce. V praxi preto môže nastať situácia, kedy zamestnávateľ bude môcť jeden zaznamenaný hovor využiť súčasne na dva rôzne účely: voči klientovi, napr. na základe jeho súhlasu na účel preukazovania zmluvného vzťahu a voči zamestnancovi, napr. na posudzovanie prípadného porušenia pracovnej disciplíny. Zamestnávateľ tak následne spracúva osobné údaje v dvoch informačných systémoch. Upozorňujeme však na zmeny, ktoré prináša nová právna úprava. V súlade s § 43 starého zákona o ochrane osobných údajov bol zamestnávateľ povinný viesť o kontrolnom mechanizme evidenciu (osobné údaje spracúval na základe osobitného zákona – Zákonníka práce) a o klientoch mohol viesť evidenciu (telefonický hovor zaznamenával na základe oso-

bitného zákona, napr. zákon o bankách) alebo bol povinný informačný systém oznámiť Úradu podľa § 33 a § 34 starého zákona o ochrane osobných údajov (telefonické hovory zaznamenával na základe súhlasu klienta).

GDPR a nový zákon o ochrane osobných údajov **rušia** v celom rozsahu oznamovaciu povinnosť k informačným systémom podľa § 33 až § 36 starého zákona o ochrane osobných údajov, ako aj povinnosť osobitnej registrácie podľa § 37 až § 41 starého zákona o ochrane osobných údajov. A povinnosť viesť evidenciu informačných systémov podľa § 43 a § 44 starého zákona o ochrane osobných údajov, t. j. povinnosť vypracovať evidenčný list bola nahradená povinnosťou viesť záznamy o spracovateľských činnostiach.

Záznamy o spracovateľských činnostiach (čl. 30 GDPR a ust. § 37 nového zákona o ochrane osobných údajov):

- vedú prevádzkovateľ, sprostredkovateľ, zástupca prevádzkovateľa/sprostredkovateľa;
- v porovnaní s evidenčnými listami informačných systémov obsahujú rovnaké údaje, pribudla „len“ povinnosť podľa možnosti uvádzať aj lehoty na vymazanie rôznych kategórií osobných údajov;
- vedú sa buď v listinnej, alebo elektronickej podobe;
- na požiadanie ich prevádzkovateľ alebo sprostredkovateľ a v príslušnom prípade zástupca prevádzkovateľa alebo sprostredkovateľa sprístupnia dozornému orgánu (Úradu);
- vzor záznamu o spracovateľských činnostiach zverejní Úrad na svojom webovom sídle.

Povinnosť viesť záznamy o spracovateľských činnostiach **sa nevzťahuje** na zamestnávateľa, ak súčasne splní všetky tieto podmienky:

- 1) má menej ako 250 zamestnancov;
- 2) nie je pravdepodobné, že spracúvanie osobných údajov, ktoré vykonáva, povedie k riziku ochrany práv a slobôd dotknutej osoby;
- 3) spracúvanie osobných údajov je príležitostné, alebo nezahŕňa osobitné kategórie osobných údajov alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky.

V okamihu splnenia vyššie uvedených podmienok (zavedenie kontrolného mechanizmu podľa § 13 ods. 4 Zákonníka práce a vymedzenia účelu jeho zavedenia pre hodnotenie plnenia povinností zo strany zamestnanca a dodržaní zásad spracúvania osobných údajov) môže zamestnávateľ použiť ako dôkazový prostriedok aj zaznamenaný telefonický rozhovor pri prípadnom pracovnoprávnom spore, predmetom ktorého je napr. porušenie pracovnej disciplíny alebo neplatné skončenie pracovného pomeru.

Iné monitorovanie hovorov zamestnancov (okrem výlučne internej komunikácie zamestnanec – zamestnanec) je v zásade nemožné a v rozpore so zákonom o ochrane

osobných údajov. Ak totiž chce zamestnávateľ monitorovať telefonický rozhovor svojho zamestnanca so zamestnancom inej spoločnosti, chýba mu na monitorovanie zamestnanca inej spoločnosti na druhej strane linky účel spracúvania osobných údajov o tejto fyzickej osobe. To, že si od tejto fyzickej osoby vypýta súhlas na monitorovanie telefonického rozhovoru, mu bez stanovenia legitímneho účelu spracúvania osobných údajov nepomôže.

K 2) Monitorovanie webovej aktivity a PC zamestnanca

Zamestnávateľ je primárne zaviazaný k určeniu podmienok, za ktorých môže zamestnanec využívať zverené pracovné pomôcky. Tieto podmienky by mali byť definované vo vnútro podnikových predpisoch, ktoré sú záväzné pre všetkých zamestnancov a zamestnanci by s nimi mali byť riadne oboznámení v zmysle § 47 ods. 2 Zákonníka práce (sú prípustné aj iné formy, zásadné je vedieť preukázať zrozumiteľné definovanie podmienok a riadne oboznámenie zamestnanca).

V súvislosti s monitorovaním webovej aktivity a PC je potrebné rovnako, ako v prípade monitorovania telefonických rozhovorov, rozlišovať dva samostatné účely spracúvania osobných údajov zamestnanca. Monitorovanie webovej aktivity a PC zamestnanca na účely bezpečnosti a ochrany dát, informácií a osobných údajov, t. j. informácie (osobné údaje) získané zamestnávateľom s cieľom zabezpečiť primeranú ochranu osobných údajov (napr. heslová politika, uchovávanie logov v rámci jednotlivých činností zamestnanca v rôznych aplikáciách, vstupy do zabezpečených priestorov a pod.) nesmie byť využívané napr. na kontrolu zamestnanca a plnenie jeho pracovných povinností. V prípade, že zamestnávateľ ním získavané informácie (osobné údaje) na účel bezpečnosti informačného systému, napr. o webovej aktivite zamestnanca, chce využiť na kontrolu efektivity využívania pracovného času a plnenia povinností zamestnanca, musí zaviesť kontrolný mechanizmus v zmysle § 13 ods. 4 Zákonníka práce.

K 3) Monitorovanie elektronickej pošty

Častým kontrolným mechanizmom je kontrola elektronickej pošty zamestnanca. Adresu elektronickej pošty zamestnanca môžeme všeobecne považovať za osobný údaj. Adresa je spravidla zložená z mena a priezviska zamestnanca a označenia spoločnosti. Aj v prípade, ak je adresa označená napr. len názvom spoločnosti (huby@firmahuby.sk) a táto adresa je v rámci komunikácie spájaná so zamestnancom, je adresa elektronickej pošty osobným údajom. Za osobný údaj by sme adresu elektronickej pošty nepovažovali len v prípade, že by ju nebolo možné spojiť so žiadnou fyzickou osobou (v praxi sa táto situácia javí ako nereálna).

Zamestnávateľ môže v rámci riadne zavedenej kontroly podľa § 13 ods. 4 Zákonníka práce vykonávať kontrolu elektronickej pošty, avšak výlučne pošty doručenej/odoslanej na/z pracovný mail (mailová adresa pridelená zamestnancovi na plnenie jeho pracovných povinností). Hranicu medzi súkromnými a pracovnými vzťahmi je zložitá defino-

vať jednoznačne.¹⁰⁴ Odporúčame zamestnávateľom pri kontrole mailovej komunikácie prijať opatrenia s cieľom zamedziť oboznámeniu sa so súkromnou korešpondenciou zamestnanca, ak bola súčasťou pracovného mailu. Zamestnanec nie je vždy schopný ovplyvniť doručenie pošty súkromného charakteru na pracovný mail. Zamestnávateľ by mal postupovať citlivo a zabezpečiť, aby nedošlo k neprimeranému zásahu do práva na súkromie zamestnanca. Opatrenia prijaté v podmienkach zamestnávateľa by mali primárne spočívať v dostatočnom poučení oprávnených osôb o spôsobe zaobchádzania so súkromnou korešpondenciou. Ak je už z predmetu správy zrejmé, že ide o súkromnú korešpondenciu, má sa zamedziť jej otvoreniu. Následne, po dohode so zamestnancom, sa má takáto korešpondencia likvidovať. Ak zamestnávateľ z dôvodu bezpečnosti a ochrany informácií (vrátane osobných údajov) automaticky archivuje všetku doručенú/odoslanú mailovú korešpondenciu, nie je povinný skúmať, či uchováva aj súkromnú korešpondenciu zamestnancov. V prípade zistenia takej skutočnosti je povinný túto korešpondenciu likvidovať vo všetkých úložiskách s ohľadom na jeho technické a personálne možnosti.

K 4) Monitorovanie polohy zamestnanca

Kontrola zamestnanca monitorovaním jeho polohy prostredníctvom SIM karty je stále viac využívaná. Poskytovatelia telekomunikačných služieb ponúkajú v rámci svojich služieb jednoduchý spôsob kontroly zamestnanca pomocou rôznych aplikácií. Pri zavádzaní kontroly musí zamestnávateľ zohľadniť podmienky, za ktorých zamestnancovi zveril pracovný prostriedok – telefón. Ak zamestnanec môže využívať mobilný telefón aj na súkromné účely, alebo má byť dostupný aj v čase, kedy neplní svoje pracovné povinnosti, musí zamestnávateľ nastaviť kontrolu polohy zamestnanca tak, aby nezasahoval do súkromia zamestnanca.

Zamestnávateľ nie je oprávnený monitorovať polohu zamestnanca v čase, kedy zamestnanec neplní svoje pracovné povinnosti (napr. po skončení pracovného času, v čase čerpania dovolenky, v čase pracovného voľna, dočasnej pracovnej neschopnosti, rehabilitácie a pod.). Zamestnávateľ je povinný zabezpečiť, že v čase, kedy si zamestnanec nebude plniť svoje pracovné povinnosti, zamestnávateľ nebude spracúvať informáciu o jeho polohe (vrátane získania takejto informácie). V praxi to znamená nastavenie aplikácie umožňujúcej prístup ku geolokalizačným službám jednotlivých SIM kariet u zamestnávateľa s väzbou na pracovný čas zamestnanca a inú pracovnú neprítomnosť zamestnanca.

Situácia, keď zamestnávateľ získal informáciu o polohe zamestnanca v čase, kedy si zamestnanec neplní pracovné povinnosti (prostredníctvom aplikácie, ktorá spravdila poskytuje informáciu o polohe SIM karty po celých 24 hodín), ale ďalej ju nevyužije, je v rozpore so zákonom o ochrane osobných údajov. Zamestnávateľ nemá legitímne

104 Bližšie: DOLOBÁČ, M.: Monitoring e-mailovej komunikácie zamestnanca v judikatúre Európskeho súdu pre ľudské práva. In: Monitorovanie zamestnancov a právo na súkromný život: zborník vedeckých príspevkov. Bratislava: Sprint dva, 2010, s. 118-126. ISBN 9788089393435.

oprávnenie na základe zavedeného kontrolného mechanizmu monitorovať polohu zamestnanca v čase, kedy si neplní svoje pracovné povinnosti (zásada obmedzenia účelu spracúvaných osobných údajov).

Obdobné pravidlá platia aj pri monitorovaní polohy zamestnanca v motorovom vozidle prostredníctvom geolokalizačných služieb. Kontrolou polohy zamestnanca nie je monitorovanie polohy motorového vozidla na základe osobitných predpisov, monitorovanie vozidla v prípade napr. krádeže alebo vedenie knihy jász prostredníctvom geolokalizačných služieb. Vedenie knihy jász prostredníctvom geolokalizačných služieb je moderným a dostupným spôsobom plnenia tejto povinnosti na daňové účely. Zamestnávateľ inštaluje do motorových vozidiel modul, ktorý sníma polohu prostredníctvom GPS a SIM karty [prostredníctvom SIM karty (internetu) sa posielajú údaje na server zamestnávateľa]. Na server sú odosielané informácie, napr. o aktuálnej rýchlosti, polohe vozidla, jeho aktuálnej spotrebe a informácia, či je jazda vykonaná na súkromné alebo služobné účely. Uvedené informácie následne zamestnávateľ spracuje a na ich základe vedie knihu jász.

Z právneho hľadiska ide o osobné údaje, ktoré je možné považovať za súčasť informačného systému „Účtovníctvo“. V prípade, že by zamestnávateľ chcel informácie využiť na kontrolu zamestnanca pri plnení jeho pracovných povinností, musel by zabezpečiť, aby do informačného systému osobných údajov „kontrola zamestnancov“ neboli odosielané údaje súvisiace s užívaním motorového vozidla v čase označenom ako „súkromná jazda“.

Bez ohľadu na spôsob monitorovania polohy zamestnanca (napr. prostredníctvom mobilného telefónu v motorovom vozidle a pod.) je zamestnávateľ povinný zabezpečiť, aby osobné údaje o polohe získaval výlučne v čase, kedy si zamestnanec plní svoje pracovné povinnosti. Možno považovať za rozporné s pravidlami ochrany osobných údajov, získavať údaje o polohe zamestnanca v čase, kedy svoje pracovné povinnosti neplní, aj za podmienky, že využíva zverený pracovný prostriedok aj na súkromné účely.

4.11. Monitorovanie priestorov a zamestnancov kamerovými systémami

Monitorovanie priestorov v podmienkach zamestnávateľa patrí medzi štandardné spôsoby ochrany majetku, bezpečnosti a kontroly zamestnancov. Monitorovanie je vždy spojené so zásahom do súkromia, do práv a právom chránených záujmov osôb, ktoré sa v monitorovanom priestore pohybujú. Zamestnávateľ musí posúdiť každý monitorovaný priestor vo vzťahu k právnemu základu a účelu, na ktorý monitorovanie zavádza, a vo vzťahu k rozsahu monitorovaného priestoru zo zreteľom na práva osôb pohybujúcich sa v monitorovanom priestore. Je nutné rozlišovať:

- a) monitorovanie priestorov prevádzky zamestnávateľa na účely ochrany majetku a bezpečnosti,
- b) monitorovanie na účely kontroly zamestnancov.

K a)

Monitorovanie priestorov prevádzky zamestnávateľa prístupných verejnosti malo svoj vlastný právny základ v ust. § 15 ods. 7 starého zákona o ochrane osobných údajov. Podľa citovaného ustanovenia, *„priestor prístupný verejnosti možno monitorovať len na účely ochrany verejného poriadku a bezpečnosti, odhaľovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia, a to len vtedy, ak je priestor zreteľne označený ako monitorovaný; monitorovaný priestor je prevádzkovateľ povinný zreteľne označiť bez ohľadu na to, či sa snímajú obraz alebo zvuk zaznamenáva na nosič informácií. Označenie monitorovaného priestoru sa nevyžaduje, ak tak ustanovuje osobitný zákon. Vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch, ak osobitný zákon neustanovuje inak“*. Novou právnou úpravou sa tento právny základ zrušil. Pokiaľ chce zamestnávateľ monitorovať vo svojej prevádzke priestory prístupné verejnosti, t. j. priestory, kde majú za dodržania stanovených podmienok prístup aj iné osoby ako zamestnanci,¹⁰⁵ alebo aj priestory, ktoré nie sú stálym pracoviskom zamestnancov,¹⁰⁶ potrebuje pre takúto spracovateľskú operáciu disponovať iným právnym základom. Rovnocenným ekvivalentom, t. j. spracúvanie sa uskutočňuje bez potreby vyžiadať si súhlas dotknutej osoby, môže byť právny základ uvedený:

- v čl. 6 ods. 1 písm. c) GDPR a čl. 13 ods. 1 písm. c) nového zákona o ochrane osobných údajov, t. j. zákonná povinnosť prevádzkovateľa; alebo
- v čl. 6 ods. 1 písm. f) GDPR a čl. 13 ods. 1 písm. f) nového zákona o ochrane osobných údajov, t. j. oprávnený záujem prevádzkovateľa.

Spracúvanie osobných údajov na účel oprávnených záujmov prevádzkovateľa nie je zákonné, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov. Takéto posúdenie môže byť pre zamestnávateľa náročné. Prvou indíciou prípustnosti monitorovania priestorov prevádzky zamestnávateľa kamerovými systémami je, že ide o priestory, v ktorých sa nachádzajú hodnoty, ktoré je potrebné chrániť pred ich poškodením, odcudzením alebo zničením (napr. nákladový priestor, sklady, dátové centrum, prístupové cesty k chráneným priestorom, chodby a spoločné priestory, ak je oprávnený dôvod na ich monitorovanie/ochranu a pod.). Zamestnávateľ môže monitorovať priestory len v rozsahu nevyhnutnom na dosiahnutie účelu, pričom platí, že pokiaľ tu existuje menej invazívny prostriedok, ktorým by zamestnávateľ dokázal chrániť svoje oprávnené záujmy, právo zamestnávateľa prevažuje nad základnými právami a slobodami dotknutých osôb. Pri monitorovaní je zamestnávateľ povinný vždy zohľadniť priestory, v ktorých má zamestnanec právo na súkromie (napr. šatne, miestnosti určené na odpočinok, toalety, sprchy a pod.).

Ako sme už uviedli (kapitola 4.10.) oznamovacia povinnosť informačných systémov, aj konanie o osobitnej registrácii boli zrušené. Miera nebezpečenstva porušenia

¹⁰⁵ Spravidla ide o priestory recepcie, vrátnice, parkoviska a pod.

¹⁰⁶ Priestory, v ktorých sa zamestnanci pohybujú iba v čase výkonu čiastkových úloh, napr. naloženie/ vyloženie tovaru, uloženie/výdaj skladových zásob a pod.

práv a slobôd dotknutých osôb, t. j. proporционаlita monitorovania priestoru vo vzťahu k právam dotknutých osôb, môže byť po novom podrobená tzv. posúdeniu vplyvu na ochranu osobných údajov (najmä ak ide o monitorovanie priestorov prístupných verejnosti vo veľkom rozsahu, čl. 35 GDPR a ust. § 42 nového zákona o ochrane osobných údajov).

GDPR vyžaduje transparentné spracúvanie osobných údajov, a tak aj naďalej platí povinnosť prevádzkovateľa monitorované priestory riadne a zreteľne označiť tak, aby osoba vstupujúca do týchto priestorov sa o monitorovaní dozvedela ešte pred okamihom vstupu do týchto priestorov. Označenie by malo byť viditeľné z dostatočnej vzdialenosti pred vstupom do monitorovaného priestoru a zrozumiteľné, pričom môže byť zložené z textu, piktogramu alebo ich kombinácie. Dotknutá osoba má právo vedieť, kto ju monitoruje a u koho si môže uplatniť svoje práva. Ak nie je z umiestnenia označenia zrejmé a zrozumiteľné, kto je prevádzkovateľom kamerového systému, je potrebné informáciu uviesť na označení. Pri monitorovaní musí zamestnávateľ dbať o to, aby monitoroval priestor len v rozsahu, ktorý zodpovedá účelu spracúvania osobných údajov (napr. pri monitorovaní parkoviska pred vstupom do areálu nemôže monitorovať príjazdovú verejnú komunikáciu). Vyhotovené záznamy môže zamestnávateľ uchovávať po primeranú dobu¹⁰⁷ a použiť ich len na stanovený účel. Ak je stanoveným účelom ochrana majetku zamestnávateľa a bezpečnosť osôb vstupujúcich do monitorovaných priestorov, nemôže zamestnávateľ záznamy použiť na iný účel, napríklad na kontrolu zamestnanca.

K b)

Podľa § 13 ods. 4 Zákonníka práce *„Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narušovať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručení na túto adresu bez toho, aby ho na to vopred upozornil.“* Citované ustanovenie predstavuje právny základ v podobe osobitného predpisu, ktorý dovoľuje monitorovanie zamestnancov na účel kontrolného mechanizmu. Monitorovanie prebieha bez súhlasu zamestnancov za dodržania jeho zavedenia v zmysle Zákonníka práce, t. j. monitorovanie na účel kontrolného mechanizmu musí byť vopred prerokované so zástupcami zamestnancov a zamestnancom musí byť poskytnutá informácia o zavádzaní kontrolného mechanizmu v súlade so Zákonníkom práce. Vyhotovené zábery môžu byť využité na vyvodenie pracovnoprávnej zodpovednosti voči zamestnancom. Monitorované môžu byť len priestory, v ktorých zamestnanci vykonávajú svoju prácu,

¹⁰⁷ Podľa ust. § 17 ods. 7 starého zákona o ochrane osobných údajov: „Ak záznam vyhotovený podľa § 15 ods. 7 nie je využitý na účely trestného konania alebo konania o priestupkoch, je ten, kto ho vyhotovil, povinný ho zlikvidovať najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený, ak osobitný zákon neustanovuje inak.“

napr. výrobná linka/hala, priestory predajne, recepcia/vstupná hala a pod., monitorovať nemožno priestory, ktoré sú na základe Zákonníka práce alebo iných zákonov určené na odpočinok, hygienu a pod. (napr. sociálne zariadenie, oddychová miestnosť, šatne).

Za predpokladu, že chce teda zamestnávateľ využiť kontrolný mechanizmus v podobe inštalácie kamier na pracovisku k hodnoteniu napr. pracovnej disciplíny zamestnancov, musí splniť vyššie uvedené podmienky jeho zavedenia a takéto monitorovanie zamestnanca za účelom kontroly pracovnej disciplíny zamestnancov sa môže uskutočňovať výlučne v právnom režime Zákonníka práce. Zamestnávateľ nemôže nahradiť tento mechanizmus v zmysle Zákonníka práce zavedením monitorovania na účel oprávnených záujmov prevádzkovateľa, hoci sa nevyklučuje, aby tieto dva systémy monitorovania boli zavedené súčasne, každý však pre iný účel a neskoršie možnosti využitia kamerových záznamov.

Na účel kontroly zamestnancov môže zamestnávateľ využiť tie isté prostriedky spracúvania osobných údajov (kamera, monitor, úložisko), ktoré už využíva na monitorovanie priestoru prevádzky na účely ochrany majetku. Rozdiely však budú v účeloch a právnych režimoch takéhoto spracúvania.

4.12 Whistleblowing

S účinnosťou od 1. januára 2015 nadobudol účinnosť nový zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov (ďalej len zákon o protispoločenskej činnosti), ktorý zaviedol tento inštitút známy z prostredia (predovšetkým amerických) nadnárodných spoločností aj do slovenského právneho prostredia. Pojem whistleblowing pochádza z anglického slovného spojenia „*blow the whistle*“ (doslova zapísať na píšťalku) a má evokovať predstavu varovnej píšťalky, ktorá zaznie, keď sa nehrá podľa pravidiel. Schválením zákona o protispoločenskej činnosti sa jednotne určilo, akým spôsobom má zamestnávateľ prijímať a vybavovať podnety týkajúce sa protispoločenskej činnosti a zároveň sa vymedzili prostriedky ochrany pre oznamovateľa.¹⁰⁸ Ide o tzv. interný whistleblowing, ktorý sa týka výlučne zamestnancov v pozícii oznamovateľov. Druhým typom whistleblowingu je tzv. externý whistleblowing, kde v pozícii oznamovateľov vystupujú externé subjekty (zákazníci, klienti, dodávatelia, spotrebiteľia, konkurenti, veritelia, študenti, pacienti a pod.). Externý whistleblowing nie je predmetom úpravy zákona o protispoločenskej činnosti.

Zamestnávateľa sú povinní zaviesť tzv. interný (vnútorný) systém vybavovania podnetov, ak zamestnávajú najmenej 50 zamestnancov. Pre ostatných zamestnávateľov je

108 Bližšie: BARINKOVÁ, M. – SEILEROVÁ, M. Ochrana oznamovateľov protispoločenskej činnosti. In: Súčasný stav a nové úlohy pracovného práva: Dies Iuris Tyrnaviensis-Trnavské právnické dni: Nová Európa-výzva a očakávaná: medzinárodná vedecká konferencia: 22.-23.9.2016, Trnava. Praha: Nakladatelství Leges, 2016, s. 83-98. ISBN 9788075021779. Tiež: BARINKOVÁ, M. – VARGA, V. – SOKOL, P. Vplyv elektronizácie na formy oznamovania protispoločenskej činnosti. In: Právo, obchod, ekonomika VII.: zborník príspevkov z vedeckého sympózia: 11. - 13. október 2017, Vysoké Tatry. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2017, s.177-192. ISBN 9788081525285.

zavedenie systému dobrovoľné. Podrobnosti o zavedenom whistleblowing mechanizme má obsahovať interný predpis vydaný zamestnávateľom, ktorý okrem iných náležitostí upravuje aj aspekty spracúvania osobných údajov uvedených v podnete.

Z pohľadu pravidiel ochrany osobných údajov tak zamestnávateľ zamestnávajúci najmenej 50 zamestnancov vytvára samostatný informačný systém, ktorého účelom je evidencia interných podnetov podľa zákona o protispoločenskej činnosti. Právnym základom pre spracúvanie osobných údajov v takomto informačnom systéme je zákonná povinnosť zamestnávateľa viesť takúto evidenciu priamo podľa zákona o protispoločenskej činnosti. Zákon o protispoločenskej činnosti diktuje aj zoznam a dobu spracúvaných osobných údajov. Evidenciu podnetov je zamestnávateľ povinný viesť počas obdobia troch rokov odo dňa doručenia podnetu, pričom z osobných údajov oznamovateľa eviduje jeho meno, priezvisko a adresu pobytu. Ak ide o anonymný podnet, uvedie sa iba poznámka, že ide o anonymný podnet. Nová právna úprava upustila od oznamovacej a registračnej povinnosti informačných systémov podľa § 33 a násl. starého zákona o ochrane osobných údajov a tie boli v plnom rozsahu zrušené. Ekvivalentom evidenčnej povinnosti informačných systémov bude za určitých podmienok vedenie záznamov o spracovateľských činnostiach (bližšie vysvetlené v kapitole 4.10.). Ak má zamestnávateľ menej ako 250 zamestnancov, spracúvanie osobných údajov oznamovateľa protispoločenskej činnosti nepovedie k riziku pre práva a slobody oznamovateľa, t. j. informačný systém evidencie podnetov je technicky a bezpečnostne chránený, zamestnávateľovi nevznikne povinnosť viesť záznam o spracovateľských činnostiach vo vzťahu k ochrane osobných údajov zamestnancov v pozícii oznamovateľov protispoločenskej činnosti.

Vo vzájomných súvislostiach whistleblowingu a ochrany osobných údajov ešte upozorňujeme, že ak zamestnávateľ na účely vybavovania podnetov podľa zákona o protispoločenskej činnosti poverí externý subjekt (tzv. zodpovedná osoba na účely zákona o protispoločenskej činnosti), je z pohľadu zákona o ochrane osobných údajov vzťah medzi zamestnávateľom a touto zodpovednou osobou, vzťahom prevádzkovateľa a sprostredkovateľa s nevyhnutnosťou regulácie ich vzájomných práv a povinností cez sprostredkovateľskú zmluvu.

V. Spracúvanie osobných údajov v kolektívnych pracovnoprávných vzťahoch (praktické prípady)

Všeobecné nariadenie o ochrane údajov i nový zákon o ochrane osobných údajov v súlade s predchádzajúcim výkladom uvedeným v podkapitole 2.2.2¹⁰⁹ menia zaužívaný právny prístup k osobnému údaju osobitnej kategórie „odborovej príslušnosti“, pričom všeobecné hodnotenie smeruje skôr k objektívnemu ambivalentnému výsledku pri zohľadnení všetkých zmien. Na jednej strane sa zjednodušuje nakladanie s citlivým údajom v podobe „odborovej príslušnosti“ zo strany oprávneného subjektu na jeho spracovanie, t. j. samotnej odborovej organizácie v zmysle čl. 9 nariadenia, na druhej strane sa sprísňuje právny režim z hľadiska spracúvania tejto informácie zo strany tretích subjektov (najmä zamestnávateľa).

5.1 Spracúvanie informácie o členstve zamestnanca v odboroch odborovou organizáciou - uplatnenie výnimky v zmysle čl. 9 ods. 2 písm. d) nariadenia

Spracúvanie informácie o členstve zamestnanca v odboroch odborovou organizáciou, ktorej je zamestnanec členom, je bezprostrednou súčasťou podstaty uvedeného členstva. Odborová organizácia musí spracúvať určitý vymedzený okruh osobných údajov zamestnancov identifikujúcich osobu zamestnanca ako fyzickej bytosti z dôvodu jeho nezameniteľnosti, vrátane ďalších citlivých údajov zamestnancov, napr. v podobe informácií o zdravotnom stave alebo okruhu rodinných príslušníkov, či ďalších informácií o osobnostných črtách a profile zamestnanca. Popísané spracúvanie osobných údajov zamestnanca, vrátane citlivých osobných údajov zamestnanca, sa odvíja od primárnej činnosti, ktorú má odborová organizácia ako zástupca zamestnancov zabezpečovať a súčasne pre naplnenie ďalších povinností, ktoré odborová organizácia musí plniť voči zamestnancovi z dôvodu jeho členstva v odborovej organizácii.

Rovnako však musíme upozorniť na skutočnosť, že predmetný výklad sa týka len väzby zamestnanca a odborovej organizácie, ktorej je zamestnanec členom. Druhá alebo ďalšia odborová organizácia, ktorá pôsobí u zamestnávateľa, takéto exkluzívne (nižšie popisované) právo na spracovanie informácie o odborovej príslušnosti zamestnanca nemá, keďže napriek tomu, že rovnako pôsobí ako odborová organizácia (zástupca zamestnancov na pracovisku), nemá právo na spracúvanie predmetnej informácie o iných zamestnancoch - členoch inej odborovej organizácie.

Pri identifikácii právneho základu, na podklade ktorého odborová organizácia, ktorej je zamestnanec členom, spracúva informáciu o jeho členstve, musíme rozlíšiť primárne účel, pre ktorý odborová organizácia túto informáciu spracúva, keďže ten sa stáva hraničným ukazovateľom aj vo vzťahu k určeniu samotného právneho základu. Bezprostredne môžeme vychádzať z premisy, že odborová organizácia, ktorej je zamestnanec členom, nemusí disponovať súhlasom zamestnanca so spracúvaním citli-

109 Bližšie k uvedenému pozri - podkapitolu 2.2.2.

vého osobného údajá v podobe jeho členstva v odborovej organizácii z dôvodu, že sa na predmetné spracúvanie osobného údajá vzťahuje výnimka obsiahnutá v čl. 9 ods. 2 písm. d) všeobecného nariadenia o ochrane osobných údajov. Predmetné ustanovenie umožňuje „*spracúvanie informácie o odborovej príslušnosti fyzickej osoby – zamestnanca, ak ho vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami združenie alebo akýkoľvek iný neziskový subjekt s odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu*“. Využitie predmetnej výnimky zo zákazu spracúvania osobného údajá osobitnej kategórie v zmysle čl. 9 ods. 2 písm. d) nariadenia umožňuje odborovej organizácii spracúvať osobné údaje osobitnej kategórie v zmysle uvedených podmienok, t. j. vždy len za predpokladu viazanosti na predmetný účel, pre ktorý je výnimka ustanovená.

Medzi uvádzané zákonné podmienky, ktorých splnenie oprávňuje odborovú organizáciu k využitiu ustanovenia čl. 9 ods. 2 písm. d) nariadenia patrí spracúvanie informácie:

- *združením alebo iným neziskovým subjektom s odborárskym zameraním,*

Právny poriadok ani pri zohľadnení novej právnej úpravy v oblasti ochrany osobných údajov explicitne nestanovuje výlučný právny režim vzniku odborovej organizácie (nevymedzuje odborovú organizáciu ako právnickú osobu s osobitným modelom založenia) a ani žiadnym iným spôsobom nevymedzuje kritériá, podľa ktorých by bolo možné bližšie rozlíšiť jednotlivé občianske združenia, ktoré majú odborový charakter, alebo ich predmetom je len ochrana záujmov zamestnancov bez väzby na príslušné ustanovenie § 11a Zákonníka práce. I naďalej tak nebude existovať hraničná línia medzi prozamestnaneckými organizáciami v pozícii občianskeho združenia a odborovými organizáciami v pozícii občianskeho združenia, ktoré si splnili povinnosť v zmysle § 230 ods. 1 Zákonníka práce a považujú sa z uvedeného dôvodu za zástupcov zamestnancov. Následne sa tak bude rozlišovať výlučne existujúci dualizmus dotýkajúci sa vzniku samotných odborových organizácií v zmysle zákona o združovaní. V prvom prípade vznikne odborová organizácia ako občianske združenie v zmysle § 9a zákona o združovaní občanov s uplatnením evidenčného princípu. Vznik odborovej príslušnosti u členov prípravného výboru nastáva okamihom zaevidovania občianskeho združenia (odborovej organizácie) na Ministerstve vnútra SR, u ostatných členov neskôr podaním prihlášky, t. j. právny režim pre spracúvanie i ochranu odborovej príslušnosti nastáva v prvom prípade okamihom zaevidovania a v druhom prípade akceptáciou prihlášky zo strany odborovej organizácie. V druhom prípade vznikne odborová organizácia, ako organizačná jednotka občianskeho združenia (odborového zväzu), s vlastnou (odvodenou) právnou subjektivitou zo stanov odborového zväzu evidovaného v Registri odborových organizácií a zamestnávateľských združení na Ministerstve vnútra SR. Právnu

subjektivitu odvádzajú jednotlivé odborové organizácie pôsobiace u zamestnávateľa od odborového zväzu za predpokladu, že sú splnené podmienky, ktoré predpokladá § 6 ods. 2 zákona o združovaní občanov, a v právnych vzťahoch vystupujú ako samostatné právne subjekty popri samotnom odborovom zväze. Ustanovenie § 6 ods. 2 zákona o združovaní občanov predpokladá, že statuty občianskeho združenia môžu určiť, ktoré organizačné jednotky občianskeho združenia majú spôsobilosť konať vlastným menom, teda i nadobúdať vlastným menom práva a povinnosti odchylné od subjektu, od ktorého odvádzajú právnu subjektivitu (t. j. odborový zväz). Právny poriadok predpokladá, že takéto organizačné jednotky musia byť v stanovách výslovne uvedené, alebo musí byť v stanovách aspoň určené, akým spôsobom sa uvedené jednotky zriaďujú, aby bolo možné zistiť, či ide v konkrétnom prípade o organizačnú jednotku vzniknutú v súlade so stanovami ako organizačnú jednotku s právnou subjektivitou. Stanovy potom musia tiež jednoznačne určiť, kto je oprávnený menom organizačnej jednotky vo všetkých veciach konať, t. j. kto je štatutárnym orgánom.¹¹⁰ Vznik odborovej príslušnosti u členov prípravného výboru základnej odborovej organizácie na podnikovej úrovni, ako organizačnej jednotky, vzniká okamihom zaevidovania tejto základnej odborovej organizácie v rámci vnútorného systému odborového zväzu a následným vydaním tzv. evidenčného listu, ako dokladu, že základná odborová organizácia predstavuje súčasť príslušného odborového zväzu. Členovia prípravného výboru sa stávajú odborovo organizovaní týmto okamihom, pričom od tohto okamihu požívajú aj právnu ochranu v súvislosti s ochranou osobných údajov.

- *v rámci svojej zákonnej činnosti odborovej organizácie,*

Právny poriadok vzhľadom na právny charakter vzniku odborovej organizácie, ako občianskeho združenia, nestanovuje obligatórny predmet činnosti odborovej organizácie obdobne, ako je to napr. v prípade obchodných spoločností. Identifikovanie „*zákonnej činnosti*“ odborovej organizácie a jej rozsah však nemožno dovodiť bezprostredne z relevantnej právnej úpravy, ale predovšetkým skôr nepriamo z historických medzinárodných dokumentov a vnútorných dokumentov samotnej odborovej organizácie. V tomto ohľade by sme s ohľadom na uplatnenie výnimky v zmysle čl. 9 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov zo spracúvania citlivých osobných údajov uprednostnili užší výklad, ktorý vymedzuje činnosť zástupcov zamestnancov (odborovej organizácie) vo väzbe na relevantné pracovnoprávne predpisy, najmä Zákonník práce, a to bez súhlasu dotknutého zamestnanca.

Generálne sa predmet činnosti odborovej organizácie v uvedenom užšom výklade bude preto v zmysle naznačeného odvádzaf tak z právneho postavenia odo-

¹¹⁰ Rozsudok Najvyššieho súdu SR z 21. februára 1997, sp. zn. 3Cdo 146/96; Rozsudok Okresného súdu Bratislava IV. z 9. marca 2010, sp. zn. 12C/209/2008; Rozsudok Okresného súdu Bratislava IV. z 8. októbra 2009, sp. zn. 24C/249/2008.

rovej organizácie, ktoré jej priznáva v § 11a ZP v podobe zástupcu zamestnancov, ako aj zo stanov a štatútu odborovej organizácie. Všeobecne možno konštatovať, že predmet zákonnej činnosti odborovej organizácie bude spočívať v zastupovaní záujmov zamestnancov v individuálnych a kolektívnych pracovnoprávných vzťahoch, vrátane kolektívneho vyjednávania, pričom bude v stanovách odborovej organizácie rozšírený o ďalšie činnosti, ktoré sú bežnou súčasťou členstva v odborovej organizácii, viažuce sa na toto zastupovanie v individuálnych a kolektívnych pracovnoprávných vzťahoch, ako je zastupovanie v právnych sporoch pred orgánmi verejnej moci v pracovnoprávnej oblasti a súdnych konaniach, poskytovanie právneho poradenstva v pracovnom práve alebo práve sociálneho zabezpečenia. Vzhľadom na chýbajúci taxatívny výpočet činností, ktoré by mala odborová organizácia zabezpečovať, bude v prípade sporu o porušenie právneho režimu ochrany osobných údajov s ohľadom na spracúvanie osobných údajov osobitnej kategórie kľúčové, aby dokázala odborová organizácia preukázať, že predmetná činnosť, pri ktorej prišlo k spracovaniu tejto kategórie osobného údajá, mala svoj právny základ v právnom predpise alebo stanovách odborovej organizácie v zmysle zákona o združovaní občanov (sporné situácie môžu nastať pri poskytovaní výhod členstva bývalým členom odborových organizácií, resp. rodinným príslušníkom členov odborových organizácií alebo v okamihu, keď príde k zdvojeniu členstva v odborových organizáciách zamestnanca, ktoré právny poriadok pripúšťa). Pri všetkých ostatných činnostiach nesúvisiacich s uvedeným výpočtom zastupovania zamestnanca v individuálnych a kolektívnych pracovnoprávných vzťahoch by sme odporúčali disponovať výslovným súhlasom zamestnanca.

- *s primeranými zárukami odborovou organizáciou,*
Spracovanie informácie o odborovej príslušnosti s primeranými zárukami predstavovalo už aj v súčasnom právnom stave pomerne významný problém zo strany odborovej organizácie, a to najmä z povahy činnosti odborovej organizácie, ktorá spravidla sídli v priestoroch zamestnávateľa, používa telekomunikačné a elektronické prostriedky poskytnuté zamestnávateľom a pod. Jednou zo základných povinností odborovej organizácie bude v rámci primeraných záruk zabezpečiť ochranu spracúvaných osobných údajov, a to prijatím primeraných bezpečnostných opatrení. Bezpečnostné opatrenia musia pokrývať všetky aspekty spracúvania osobných údajov, t. j. osobné údaje vo všetkých formách ich spracúvania musia byť chránené technickými, organizačnými a personálnymi opatreniami, ktorých cieľom je zabrániť neoprávnenému spracúvaniu osobných údajov. Prijatie primeraných bezpečnostných opatrení závisí od podmienok, v ktorých odborová organizácia osobné údaje spracúva. Odborová organizácia spravidla pôsobí v priestoroch zamestnávateľa. Z hľadiska prijatia primeraných bezpečnostných opatrení treba zohľadniť, či priestory, v ktorých spracúva osobné údaje o členoch možno v dostatočnej miere oddeliť od ostatných priesto-

rov zamestnávateľa, a to tak mechanicky (napr. dvere, kľúče, mreže a iné mechanické zábranné prostriedky), ako aj automatizovanou formou spracúvania osobných údajov (napr. pracovné stanice, server, prístup na internet, použitý hardvér a softvér a pod.). Od podmienok, v akých odborová organizácia spracúva osobné údaje, bude závisieť, aké bezpečnostné opatrenia bude povinná prijať a v akom rozsahu. Odborová organizácia v takom prípade musí sama prijať primerané bezpečnostné opatrenia vo vzťahu k spracúvaným osobným údajom. Pri uvádzaní bezpečnostných opatrení treba zohľadniť aj tie bezpečnostné opatrenia, ktoré už prijal zamestnávateľ na zabezpečenie ochrany osobných údajov [napr. bezpečnostná služba, existencia kamerového informačného systému, požiarne opatrenia, podmienky BOZP, heslová politika, kľúčová politika, hardvér a softvér (ak ho pri svojej činnosti využíva), podmienky pohybu osôb v priestoroch a pod.]. O bezpečnostných opatreniach prijatých zamestnávateľom má byť informovaný každý zamestnanec v rozsahu nevyhnutnom na výkon jeho pracovných činností.

Primárne sa členovia odborovej organizácie musia riadiť bezpečnostnými opatreniami prijatými zamestnávateľom na ochranu osobných údajov (to platí vždy, ak odborová organizácia pôsobí v priestoroch zamestnávateľa). V tomto prípade primárnu zodpovednosť za osobné údaje spracúvané aj na účely členstva v odborovej organizácii nesie zamestnávateľ. Odborová organizácia má minimálnu možnosť ovplyvniť prijaté bezpečnostné opatrenia, napr. vo vzťahu k ochrane osobných údajov pred škodlivým kódom, reguláciu prístupu oprávnených osôb k serveru, rozsah ich oprávnení a pod. Nastáva neštandardná situácia, kedy vo vzťahu k spracúvaným osobným údajom, vrátane osobitnej kategórie, musí prijať primerané bezpečnostné opatrenia rovnako zamestnávateľ aj odborová organizácia, každý v rozsahu podmienok, za akých osobné údaje spracúva. Zamestnávateľ je napr. povinný zabezpečiť, aby k osobným údajom spracúvaným na dátových úložiskách, ktoré využíva zároveň aj odborová organizácia, mali prístup len oprávnené osoby, a to len v rozsahu, ktorý zodpovedá ich pracovnému zaradeniu, príp. plneniu pracovných úloh. Pre zamestnávateľa vzniká náročná situácia chrániť osobné údaje, ktoré de facto nechce a ani nemá spracúvať. No ich uchovávanie na dátovom úložisku je spracovateľskou operáciou. Z aplikačnej praxe Úradu vyplýva, že túto neštandardnú situáciu rešpektuje s ohľadom na postupy prijaté zamestnávateľom vo vzťahu k spracúvaniu osobných údajov o členstve v odborovej organizácii, s cieľom zamedziť prístup neoprávnených osôb k týmto údajom. Zároveň platí, že odborová organizácia musí prijať primerané bezpečnostné opatrenia v rozsahu, ktorý nepokrýva primerané bezpečnostné opatrenia zamestnávateľa.

Prijatie primeraných bezpečnostných opatrení spočíva v systéme mechanizmov, ktoré sa dotýkajú všetkých oblastí spracúvania osobných údajov (musia zohľadniť všetky situácie, počnúc vstupom do objektu, prístupom k osobným údajom,

bezpečnosťou vo virtuálnom priestore, ochranou samotného objektu až po ich bezpečnú likvidáciu). Osobné údaje musia byť chránené pri všetkých spracovateľských operáciách a tomu musia zodpovedať aj bezpečnostné opatrenia.

- *odborovou organizáciou iba len o členoch, alebo bývalých členoch, alebo tých fyzických osobách, ktoré majú s ňou pravidelný kontakt vzhľadom na jej ciele,*

Nový zákon o ochrane osobných údajov a nariadenie sa v rámci osobného rozsahu tohto právneho základu do určitej miery rozchádzajú. Nariadenie vymedzuje okruh osôb, o ktorých odborovú príslušnosť v uvedenom rozsahu ide širšie, ako to uvádza nový zákon o ochrane osobných údajov. V prípade nového zákona o ochrane osobných údajov sa predpokladá, že informácia o odborovej príslušnosti bude spracúvaná u členov odborovej organizácie a u tých fyzických osôb, ktoré sú s odborovou organizáciou vzhľadom na ich ciele v pravidelnom styku. V prípade druhej kategórie osôb pôjde pravdepodobne o osoby, ktoré sú rodinnými príslušníkmi členov odborovej organizácie, keďže aj v prospech nich na základe stanov odborovej organizácie si môže odborová organizácia plniť svoje povinnosti vyplývajúce z členstva (napr. právne poradenstvo), ale pravdepodobne aj osoby, ktoré sa nejakým spôsobom podieľajú na zabezpečovaní jednotlivých činností odborovej organizácie. Nariadenie v čl. 9 ods. 2 písm. d) uvádza ako okruh osôb, o ktorých je možné spracúvať informáciu o odborovej príslušnosti, aj bývalých členov odborovej organizácie, čo je pochopiteľné z hľadiska existujúcej aplikačnej praxe, kde zostávajú zachované v systémoch odborovej organizácie aj informácie o bývalých členoch pre možnosť prípadného obnovenia členstva a z neho plynúcej možnosti započítania doby pôvodne ukončeného členstva z dôvodu čerpania benefitov, odvíjajúcej sa od dĺžky členstva zamestnanca v odborovej organizácii.

- *odborová organizácia výlučne pre svoju vnútornú potrebu, a*

Obdobne, ako v prípade zákonnej činnosti odborovej organizácie, sa okruh činností spadajúcich do vnútornej potreby odborovej organizácie bude odvíjať od stanov odborovej organizácie a od jej vnútroodborových dokumentov (napr. zásady hospodárenia, štatút odborovej organizácie a pod.) rovnako s previazaním na jej činnosť zastupovania v individuálnych a kolektívnych pracovnoprávných vzťahoch v spomínanom užšom výklade. Predmetom vnútornej potreby tak bude analogicky spracúvanie informácie o členstve pre plnenia povinností vyplývajúce z vnútroodborových dokumentov (napr. platenie členského príspevku), poskytovanie právneho poradenstva a zastupovanie pred súdmi a orgánmi verejnej moci a pod.

- *bez ich poskytnutia tretej strane bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby.*

Vzhľadom na povahu spracúvaného osobného údajá osobitnej kategórie nariadenie explicitne zakazuje poskytovanie informácie o odborovej príslušnosti zamestnancov tretím osobám zo strany odborovej organizácie s výnimkou prí-

padu, ak by sám zamestnanec udelil písomne alebo hodnoverne preukázateľným spôsobom súhlas. Udelenie súhlasu sa dá predpokladať v prípadoch, kedy odborová organizácia bude zastupovať zamestnanca v prípadoch vyplývajúcich z členstva v odborovej organizácii, napr. v rámci rôznych sociálnych výpomocí alebo sociálnej starostlivosti, kedy sa vyžaduje participácia tretieho subjektu, pričom informácia o odborovej príslušnosti zamestnanca je v uvedenej situácii podstatná.

Právotvorným prvkom, ktorý bude príčinnou súvislosťou uplatnenia výnimky v zmysle čl. 9 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov, bude prihláška dotknutej osoby (zamestnanca) do odborovej organizácie, t. j. že sa zamestnanec chce stať členom odborovej organizácie na dobrovoľnom princípe. Prihláška za člena odborovej organizácie spravidla obsahuje informácie o osobe zamestnanca v rozsahu mena a priezviska, adresy trvalého bydliska, názvu podniku (pracoviska), pracovného zaradenia, dátumu narodenia, telefónneho a emailového kontaktu či samotného podpisu zamestnanca. Zoznam osobných údajov bude zodpovedať účelu spracúvania, ktorým je členstvo v odborovej organizácii, vrátane výkonu práv a povinností vyplývajúcich z tohto členstva, pričom v tomto ohľade sa uplatní nariadením určený rozsah zákonnej činnosti odborovej organizácie a spracúvanie tejto informácie o odborovej príslušnosti pre vnútornú potrebu odborovej organizácie. Nakladanie s týmto údajom musí preto plne rešpektovať a vychádzať zo stanov odborovej organizácie a ďalších vnútroorganizačných aktov, ktoré by mali vymedzovať spôsoby a situácie nakladania s takouto informáciou o zamestnancovi vo vzťahu k jeho členovi (účel spracúvania, rozsah, spôsoby a pod.). Súčasťou prihlášky za člena odborovej organizácie býva i deklarácia (vyhlásenie) zamestnanca o tom, že bude platiť členské príspevky odborovej organizácii, najčastejšie formou dohody o zrážkach zo mzdy. Dohoda o zrážkach zo mzdy býva pravidelne pripojená k samotnej prihláške do odborovej organizácie, čím si odborová organizácia zabezpečuje automaticky vylúčenie možnosti vzniku neplatičov.

5.2 Spracúvanie informácie o členstve zamestnanca v odboroch odborovou organizáciou - súhlas zamestnanca čl. 9 ods. 2 písm. a) nariadenia

Špecifickým prípadom, v rámci ktorého by sa podľa nášho názoru nemala uplatniť výnimka spracúvania citlivých údajov zamestnanca odborovou organizáciou, v uvedenom prípade informácie o odborovej príslušnosti zamestnanca, by malo byť spracúvanie citlivého údaja o odborovej príslušnosti pre účel zabezpečenia sociálnych podpôr alebo benefitov pre členov vyplývajúcich z ich členstva v odborovej organizácii. Vychádzame totiž najmä z dvoch predpokladov, pričom prvý sa odvíja už od spomínanej základnej činnosti odborovej organizácie, ako formy zastúpenia zamestnancov na pracovisku v zmysle § 11a Zákonníka práce a z druhého predpokladu, ktorý spočíva

v možnosti zamestnanca ovplyvniť poskytnutie informácie o jeho členstve v odborovej organizácii tretím subjektom.

Z vyššie uvedeného výkladu možno dovodiť základnú premisu, že základnou činnosťou odborovej organizácie by malo byť zastupovanie zamestnanca v individuálnych a kolektívnych pracovnoprávných vzťahoch v zmysle § 232 ods. 2 Zákonníka práce, ktoré sa prejavuje najmä formou právnej pomoci alebo podpory, napr. pri uplatňovaní jednotlivých pracovnoprávných inštitútov (prerokovanie skončenia pracovného pomeru, posúdenie, či ide o neospravedlnené zameškanie zmeny, vyšetrovanie príčin škody na zdraví formou pracovného úrazu alebo choroby z povolania a pod.). Odborové organizácie sa však v ostatnom období výraznejšie posunuli od klasickej formy zastupovania zamestnancov, ako súčasti členstva, k zabezpečeniu ďalších činností, ktoré si ich členovia vyžadovali, alebo by im boli prospešné, a to najmä formou vytvárania sociálneho fondu odborovej organizácie tvoreného z členských príspevkov odborovej organizácie slúžiacej k poskytovaniu rôznych sociálnych výpomocí alebo dotovania sociálnych programov pre členov. Typickými príspevkami v rámci spomínanej sociálnej výpomoci sa tak stávajú podpora pri narodení dieťaťa, podpora pri úmrtí rodinného príslušníka, alebo priamo člena odborovej organizácie, podpora pri dlhodobej alebo krátkodobej dočasnej pracovnej neschopnosti, podpora na letné alebo zimné dovolenky, regeneráciu pracovných síl a pod. Obdobným spôsobom sú však podporované aj ďalšie formy benefity členstva v odborovej organizácii, napr. dotácie na rôzne kultúrne podujatia, lístky do zábavných zariadení a pod. Hoci uvedené činnosti odborovej organizácie môžeme vnímať pozitívne z pohľadu marketingu odborovej organizácie alebo celkovej starostlivosti o člena, pri zasadení do kontextu dôvodu skutočného vzniku a existencie odborovej organizácie, ako zástupcu zamestnancov na pracovisku, by takéto rozširovanie „činnosti“ odborovej organizácie bolo príliš extenzívne. A to aj v prípade, pokiaľ by boli tieto činnosti uvedené vo vnútroodborových dokumentoch odborovej organizácie.

Pokiaľ by sme dali do vzájomného pomeru uplatnenie výnimky v zmysle čl. 9 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov, ktorá umožňuje spracúvať citlivé údaje zamestnancov bez ich súhlasu, s možným bezbrehým a extenzívnym výkladom činnosti odborovej organizácie (čo by mala zabezpečovať pre svojich členov), zdá sa nám, že by tu existoval zásadný nepomer v neprospech zamestnancov z pohľadu narušenia konceptu ochrany ich osobných údajov vo vzťahu k rozšíreniu katalógových účelov, pre ktoré sú tieto údaje spracúvané.

Druhý predpoklad neuplatnenia výnimky v zmysle § 9 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov spočíva v nesplnení poslednej podmienky naplnenia výnimky uvádzaného ustanovenia v podobe, že odborová organizácia *“neposkytne tretej strane bez písomného alebo inak hodnoverne preukázateľného súhlasu dotknutej osoby”* informáciu o odborovej príslušnosti zamestnanca. Podstatou benefitného systému je uzatváranie zmlúv s tretími subjektmi, ktoré vykonávajú svoju činnosť či už v oblasti zábavného priemyslu, služieb a pod., predmetom ktorých je poskytnutie zľavy alebo iného zvýhodneného tovaru alebo služby, práve členom odborovej organizácie. K zabezpeče-

niu efektívneho fungovania tohto systému sa však vyžaduje, aby sa takémuto zmluvnému partnerovi poskytla databáza členov odborovej organizácie, aby sa na jednej strane mohol presvedčiť o oprávnenosti poskytnutia tejto zľavy fyzickej osobe, na druhej strane, aby bola zabezpečená efektivita a účelnosť systému z pohľadu jeho aktualizácie, keď nárok na zľavy strácajú fyzické osoby, ktoré prestali byť členmi odborovej organizácie. Hoci vo väčších odborových organizáciách je systém založený na jedinečnom čísle pre každého zamestnanca, ktoré sa poskytne zmluvnému partnerovi a prostredníctvom ktorého dokáže identifikovať fyzickú osobu v okamihu, keď sa dožaduje zľavy v jeho zariadení, v menších odborových organizáciách sa poskytujú zmluvným partnerom priamo identifikačné údaje členov v rozsahu meno, priezvisko a niekedy aj rodné číslo, pričom jednoznačne prichádza k určeniu fyzickej osoby za člena odborovej organizácie a k spracúvaniu informácie o odborovej príslušnosti zamestnanca treťou osobu bez jeho súhlasu. Nadôvažok musíme pripomenúť, že zamestnanec - člen odborovej organizácie ako jednotlivec nemá možnosť zamedziť získaniu konkrétneho benefitu tým, že by s jeho zavedením vyslovil nesúhlas. Teoreticky je síce možné, aby vyjadril nesúhlas s poskytnutím svojich osobných údajov takejto tretej strane, v aplikačnej praxi však zamestnanec netuší, akým spôsobom je zabezpečené preukazovanie členstva v odborovej organizácii u tohto obchodníka a ani nevie jeho vnútorné fungovanie, keďže to sa spravidla líši v závislosti od typu benefitu a samotnej tretej strany.

Domnievame sa preto, že v uvádzaných prípadoch nesplnenia podmienok výnimky v zmysle § 9 ods. 2 písm. d) všeobecného nariadenia o ochrane údajov, by mal byť jediným právnym základom pre spracovanie citlivých údajov o zamestnancoch výlučne udelený súhlas z ich strany v zmysle § 9 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov z pohľadu všetkých spomenutých účelov, pre ktoré odborová organizácia spracúva informáciu o odborovej príslušnosti zamestnanca.

Pre udelenie súhlasu dotknutej osoby sa následne uplatní právny režim § 9 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov, t. j. že zamestnanec udelil odborovej organizácii výslovný súhlas so spracúvaním osobných údajov osobitnej kategórie na účel poskytovania sociálnych výpomocí alebo zavedeného benefitného systému. Získanie tohto súhlasu by si mala zabezpečiť sama odborová organizácia pri vstupe zamestnanca do svojej členskej základne, resp. najneskôr pred tým, ako začne využívať niektorý z benefitov alebo čerpať sociálnu výpomoc. Odporúča sa samozrejme vytvoriť osobitný formulár, v ktorom budú v zmysle vyššie uvedeného výkladu obsiahnuté všetky relevantné informácie, ktorými by mal zamestnanec disponovať pred udelením takéhoto súhlasu, a to najmä účel spracúvania, rozsah spracúvania, doba spracúvania osobných údajov a pod., vrátane možnosti odvolať udelený súhlas.

5.3 Spracúvanie osobných údajov odborovo organizovaného a odborovo neorganizovaného zamestnanca odborovou organizáciou

Osobitosť postavenia odborovej organizácie v pracovnoprávných vzťahoch na rozdiel od ostatných subjektov dotvára i rozsah oprávnení a kompetencií, ktoré jej priznáva

Zákonník práce a ostatné pracovnoprávne predpisy. Na základe tohto právneho režimu prichádza k ďalšiemu spracúvaniu osobných údajov odborovou organizáciou pri výkone funkcie zástupcu zamestnancov podľa § 11a Zákonníka práce. Právny základ spracúvania osobných údajov v tomto prípade predstavuje podľa čl. 6 ods. 1 písm. c) nariadenia a alternatívne i § 13 nového zákona o ochrane osobných údajov a v niektorých prípadoch opätovne § 9 ods. 2 písm. d) nariadenia, keďže v tomto prípade prichádza k splneniu zákonnej povinnosti prevádzkovateľa (napr. § 74 Zákonníka práce), ktorú stanovujú osobitné pracovnoprávne predpisy, a spracúvanie osobných údajov aj o odborovej príslušnosti je realizované aj vo väzbe na § 232 ods. 2 a § 232 ods. 3 Zákonníka práce.

Spracúvanie takýchto osobných údajov odborová organizácia realizuje v osobitne zriadenom internom informačnom systéme, keďže rozsah osobných údajov je nepomerne širší, ako v prípade interného informačného systému evidencie členstva s ohľadom na rozsah zákonných kompetencií zástupcov zamestnancov v zmysle osobitných pracovnoprávných predpisov. Rozsah spracúvaných údajov je variabilnejší a mení sa s ohľadom na výkon jednotlivých kompetencií, ktoré odborová organizácia vykonáva v zmysle príslušných pracovnoprávných predpisov (od výkonu kontrolnej činnosti podľa § 239 ZP, kde sa spracúvajú informácie o mzdových a pracovných podmienkach zamestnancov, informácie o skončení pracovnoprávneho vzťahu až po osobné údaje dotýkajúce sa zdravotného stavu pri vyšetrovaní pracovného úrazu, preventívnych zdravotných prehliadok a pod.).

Vo vzťahu k výkonu jednotlivých kompetencií, ktoré Zákonník práce alebo iné pracovnoprávne predpisy priznávajú zástupcom zamestnancov, môže prichádzať k spracúvaniu rôzneho rozsahu osobných údajov zamestnancov, aj odborovo neorganizovaných. Rozsah týchto osobných údajov nie je možné vopred odhadnúť a ich štruktúra a zoznam bude závisieť od konkrétnej situácie. Získavanie takýchto osobných údajov od zamestnávateľa alebo tretích subjektov a ich neskoršia ochrana bude závislá od relevantnej právnej úpravy obsiahnutej v osobitných právnych predpisoch a od účelu výkonu kompetencie zo strany odborovej organizácie, napr. vo väzbe na § 232 ods. 3 Zákonníka práce a vo väzbe na čl. 6 ods. 1 písm. c) nariadenia. Na účely pracovnoprávných vzťahov a výkonu kompetencií zo strany odborovej organizácie bude východiskový právny rámec predstavovať najmä § 238 a § 239 Zákonníka práce, kde v rámci aplikačnej praxe prichádza najčastejšie k požiadavke odborovej organizácie získať od zamestnávateľa informácie, ktoré môžu potenciálne predstavovať osobné údaje fyzických osôb.

Právnym základom pre spracúvanie osobných údajov zamestnancov bez ich súhlasu, odborovo aj neodborovo organizovaných, bude teda právny predpis minimálne so silou zákona (osobitný predpis v zmysle terminológie všeobecného nariadenia o ochrane údajov a nový zákon o ochrane osobných údajov) alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná. Logická súslednosť sa však vždy bude odvíjať od skutočnosti, či zamestnanec je odborovo organizovaný alebo nie, keďže v § 232 ods. 3 Zákonníka práce sa umožňuje úplne vylúčiť pôsobnosť akejkoľvek formy zastúpenia

zamestnancov na pracovisku. Pokiaľ teda bude zamestnanec odborovo organizovaný, automaticky sa uplatní zastupovanie odborovou organizáciou v individuálnych pracovnoprávných vzťahoch, pričom spracúvanie ďalších osobných údajov o zamestnancovi bude dané charakterom pracovnoprávného inštitútu, v ktorom sa má zastupovanie odborovou organizáciou uskutočniť. V prípade odborovo neorganizovaného zamestnanca však takýto automatický postup uplatniť nemožno, keďže v zmysle § 232 ods. 3 Zákonníka práce má zamestnanec odborovo neorganizovaný určiť iný post svojho zastupovania v individuálnych pracovnoprávných vzťahoch ako predvída Zákonník práce (takéhoto zamestnanca by mala v individuálnych pracovnoprávných vzťahoch zastupovať odborová organizácia s najväčším počtom členov u zamestnávateľa). Zamestnanec má možnosť určiť, že ho zastúpi iná odborová organizácia (logicky s nižším počtom zamestnancov u zamestnávateľa), alebo že sa zastúpi sám. V takomto prípade sa vôbec nemusí automaticky uplatniť výnimka zo spracúvania osobných údajov bez súhlasu dotknutého zamestnanca.

Až po vyriešení tejto premisy o odborovej organizovanosti zamestnanca môže prísť ku konkretizácii rozsahu spracúvaných osobných údajov zamestnanca, t. j. pri spracúvaní osobných údajov na základe tohto právneho základu je prevádzkovateľ (odborová organizácia) viazaný povinnosťou spracúvať osobné údaje len v rozsahu a spôsobom, ktorý tento osobitný predpis alebo medzinárodná zmluva ustanovuje. Prevádzkovateľ je teda oprávnený spracúvať len také osobné údaje, ktoré sú priamo vymedzené osobitným predpisom alebo medzinárodnou zmluvou (uvádzaný zoznam osobných údajov) alebo také osobné údaje, ktoré sú nevyhnutné na dosiahnutie osobitným zákonom alebo medzinárodnou zmluvou stanoveného účelu (rozsah osobných údajov).¹¹¹ Typickým príkladom môže byť napríklad prerokovanie skončenia pracovného pomeru podľa § 74 Zákonníka práce, keď sa v závislosti od podmienok konkrétneho prípadu môžu líšiť informácie, ktoré je nevyhnutné spracovať pre možnosť uskutočnenia inštitútu prerokovania výpovede alebo okamžitého skončenia pracovného pomeru zamestnanca. Ak vychádzame z jednotlivých výpovedných dôvodov podľa § 63 Zákonníka práce alebo dôvodov pre okamžité skončenie pracovného pomeru, charakter údajov bude postupovať od konkretizácie prípadov menej závažného alebo závažného porušenia pracovnej disciplíny (informácie o zdravotnom stave pri alkoholizme alebo omamných a psychotropných látkach), až po informácie dotýkajúce sa nespôsobilosti zamestnanca na výkon doterajšej práce, prípadne informácie o skutočnostiach, pre ktoré bol zamestnanec odsúdený pre úmyselný trestný čin a možno s ním okamžite skončiť pracovný pomer).

111 Napr. čl. 11 Zákonníka práce (osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával).

5.4 Realizácia zrážok zo mzdy a spracúvanie informácie o členstve zamestnanca v odborovej organizácii zamestnávateľom

Osobitným prípadom, pri ktorom prichádza najčastejšie k sporom medzi odborovou organizáciou a zamestnávateľom ohľadom spracovania osobitnej kategórie osobného údajov v podobe odborovej príslušnosti, je zrážanie členského príspevku prostredníctvom zamestnávateľa. Častým príkladom v praxi je situácia, kedy odborová organizácia, ako súčasť členstva fyzickej osoby – zamestnanca, vyberá určitý členský príspevok za neskôr poskytované služby v podobe zastupovania v súdnych konaniach, kolektívnom vyjednávaní alebo právnej pomoci voči zamestnávateľovi. Členský príspevok predstavuje spravidla stanovené percento z čistej mzdy zamestnanca. Vyberanie členského príspevku sa uskutočňuje rôznymi spôsobmi od trvalého príkazu v banke, až po najčastejší spôsob v podobe zrážky zo mzdy zamestnanca.

Spôsob zrážania členského príspevku zo mzdy predstavuje najistejší a najjednoduchší spôsob vyberania členského príspevku pre odborovú organizáciu, keďže na jednej strane administratívne náklady a istotu zrazenia zaisťuje zamestnávateľ (dohodu o zrážkach zo mzdy podpisuje zamestnanec už ako súčasť prihlášky v prospech odborovej organizácie). Súčasne sa odborová organizácia vyhne vzniku neplatenia členských príspevkov, keďže ten už je neskôr v procese výberu automatizovaný a prebieha bez súčinnosti zamestnanca v mzdovom systéme zamestnávateľa. Odborová organizácia tak napr. nemusí obchádzať zamestnancov a vyberať od nich členský príspevok fyzicky, alebo sa vyhne zrušeniu trvalého príkazu zamestnancom z rôznych subjektívnych alebo objektívnych dôvodov. Zamestnávateľ realizuje uvedený spôsob výberu členského tak, že každému zamestnancovi vykoná na základe dohody o zrážke zo mzdy zrážku a úhrnnú sumu zrážok z miezd zamestnancov (členov) poukáže jedným príkazom na úhradu na účet odborovej organizácie.

Hoci v minulosti predstavovali dohody o zrážkach zo mzdy spornú oblasť vzájomného vzťahu medzi zamestnancom i zamestnávateľom, keďže zamestnávatelia mali tendenciu brániť sa zvýšeným nákladom na túto činnosť v okamihu, keď u niektorých zamestnancov realizovali niekoľko takýchto zrážok, v súčasnosti sa tento problém dostal skôr do polohy už len istej nátlakovej hry zamestnávateľa na odborovú organizáciu, keď mu tá nevychádza v ústrety pri jeho požiadavkách pri uplatňovaní jednotlivých pracovnoprávných inštitútov. Bezprostredne však musíme uviesť, že odborová organizácia má právo od zamestnávateľa takéto zrážanie členských príspevkov požadovať pri splnení určitých zákonom vyžadovaných predpokladov, ktoré sú predmetom neskoršieho výkladu.

Právnym základom pre realizáciu takejto zrážky zo mzdy je dohoda o zrážkach zo mzdy, ktorú v zmysle § 131 ods. 3 Zákonníka práce uzatvára zamestnanec spolu so zamestnávateľom, a to z dôvodu, že v zmysle § 131 ods. 3 Zákonníka práce ďalšie zrážky zo mzdy, ktoré presahujú rámec zrážok uvedených v odsekoch 1 a 2, môže zamestnávateľ vykonávať len na základe písomnej dohody so zamestnancom o zrážkach zo mzdy, alebo ak povinnosť zamestnávateľa vykonávať zrážky zo mzdy a iných príjmov zamest-

nanca vyplýva z osobitného predpisu. Zákonník práce a ani žiadny iný pracovnoprávny predpis neustanovuje formálne alebo obsahové náležitosti takejto dohody o zrážkach zo mzdy. Predpokladá sa však, že táto dohoda o zrážkach zo mzdy, ako dvojstranný právny úkon, by mal spĺňať formálne požiadavky, ktoré na dvojstranné právne úkony kladie Občiansky zákonník.

V tomto ohľade sa však z hľadiska aplikačnej praxe odporúča, aby dohoda o zrážkach zo mzdy neobsahovala explicitný účel, pre ktorý je vykonávaná zrážka zo mzdy z dôvodu ochrany odborovej príslušnosti zamestnanca, ako osobného údaja osobitnej kategórie. Postačuje, pokiaľ dohoda o zrážkach zo mzdy obsahuje označenie bankového účtu, v prospech ktorého má byť táto zrážka zo mzdy zamestnanca realizovaná a uvedenie výšky zrážky zo mzdy zamestnanca. Načrtnutá anonymizácia neslúži len na ochranu odborovej príslušnosti zamestnanca, ale súčasne vychádza v ústrety aj spracúvaniu predmetnej kategórie osobného údaja osobitnej kategórie z pohľadu princípu primeranosti. Napriek skutočnosti, ak by aj v tejto dohode o zrážkach zo mzdy bol taxatívne uvedený účel, pre ktorý sa zrážka zo mzdy realizuje, nespôsobuje to apriori právny záver, že zamestnávateľ spracúva informáciu o odborovej príslušnosti zamestnanca. To však len za predpokladu, že zrážka je realizovaná na podklade tejto dohody o zrážkach zo mzdy uzatvorenej medzi zamestnávateľom a zamestnancom, ktorá tvorí aj právny základ pre účely všeobecného nariadenia o ochrane údajov a nového zákona o ochrane osobných údajov. V tomto prípade by právny základ tvoril samotný súhlas zamestnanca v zmysle čl. 7 a čl. 9 všeobecného nariadenia o ochrane údajov.

Súčasne sa však vyžaduje naplnenie predpokladu, že zamestnávateľ cielené nespracúva informáciu o odborovej príslušnosti zamestnanca na vopred určený účel v podobe spracúvania osobného údaju osobitnej kategórie o odborovej príslušnosti na iný účel, než je realizácia zrážky zo mzdy. Hoci sa teda zamestnávateľ „nepriamo“ dostane k informácii, že zrážka zo mzdy je realizovaná za účelom výberu členského príspevku v prospech konkrétnej odborovej organizácie, nie je jeho zamýšľaným cieľom túto informáciu spracúvať, napr. s cieľom jej neskoršieho použitia v pracovnoprávných vzťahoch.

Zamestnávateľ túto informáciu „nepriamo“ spracúva spravidla ako súčasť mzdovej agendy, v rámci spracovateľských činností súvisiacich s realizáciou personálnej a mzdovej agendy. Preto sa od neho vyžaduje, aby takéto osobné údaje osobitnej kategórie o zamestnancoch chránil (primerané záruky) a súčasne ich on sám nevyužíval v pracovnoprávných vzťahoch pozitívnym alebo negatívnym spôsobom. V uvedenom prípade by sme sa dostávali už do rozporu s čl. 1 Základných zásad Zákonníka práce a súčasne § 13 Zákonníka práce, ktorý zakazuje diskrimináciu zamestnanca z dôvodu jeho odborovej príslušnosti. Zohľadňujeme pritom skutočnosť, že Zákonník práce a ani žiadny iný pracovnoprávny predpis (bez zohľadnenia právneho režimu ochrany osobných údajov) explicitne nezakazuje spracúvanie informácie o odborovej príslušnosti zamestnanca, len zakazuje zamestnávateľovi v zmysle uvedených ustanovení diskriminovať (porušiť zásadu rovnakého zaobchádzania) zamestnanca pri realizácii pracovnoprávných vzťahov.

Vykonávanie zrážok zo mzdy zamestnancov predstavuje základnú súčasť procesu výberu členského príspevku prostredníctvom dohôd o zrážkach zo mzdy. V niektorých prípadoch však odborové organizácie vyžadujú od zamestnávateľa ešte aj vytvorenie menného zoznamu zamestnancov, u ktorých bola v príslušnom mesiaci takáto zrážka zo mzdy vykonaná práve z dôvodu, aby si vedeli skontrolovať, či si ich člen splnil základnú povinnosť spočívajúcu v platení členského príspevku. Hoci do súčasnosti predstavovalo vyhotovenie tohto zoznamu právne spornú oblasť vzájomných vzťahov medzi odborovou organizáciou a zamestnávateľom, nariadenie prináša v uvedenej oblasti do značnej miery významný posun. Relevantnými ustanoveniami v tomto prípade môžu byť ustanovenia čl. 88 v spojení s čl. 9 ods. 2 písm. b) nariadenia, ktoré umožňujú „členským štátom prostredníctvom právnych predpisov alebo **kolektívnych dohôd** stanoviť konkrétnejšie pravidlá na zabezpečenie ochrany práv a slobôd pri spracúvaní osobných údajov zamestnancov v súvislosti so zamestnaním, najmä na účely prijatia do zamestnania, plnenia pracovnej zmluvy, vrátane plnenia povinností vyplývajúcich z právnych predpisov alebo kolektívnych zmlúv, ďalej na účely riadenia, plánovania a organizácie práce, rovnosti a rozmanitosti na pracovisku, ochrany zdravia a bezpečnosti pri práci, ochrany majetku zamestnávateľa alebo zákazníka, ako aj na účely uplatňovania a využívania práv a výhod súvisiacich so zamestnaním na individuálnom alebo kolektívnom základe a na účely ukončenia pracovného pomeru“ a ďalej uplatnenie výnimky zo zákazu spracúvania osobných údajov osobitnej kategórie v zmysle čl. 9 ods. 1 nariadenia v okamihu, keď je „spracúvanie nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu, poskytujúce primerané záruky ochrany základných práv a záujmov dotknutej osoby“.

Nariadenie v uvádzaných ustanoveniach článkov tak pripúšťa možnosť zamestnávateľa a odborovej organizácie dohodnúť sa na ustanovení povinnosti pre zamestnávateľa na jednej strane vykonávať zrážky zo mzdy a súčasne po ich realizácii zamestnávateľom vyhotovovať menný zoznam zamestnancov, u ktorých bola takáto zrážka zo mzdy zrealizovaná. Táto povinnosť bude súčasťou stanovenia konkrétnejších pravidiel na ochranu osobných údajov zamestnancov v spojení s nevyhnutnosťou spracúvania týchto osobných údajov osobitnej kategórie v súvislosti so zamestnaním a plnením povinnosti zamestnávateľa stanovenej kolektívnou zmluvou, ako prípustným právnym základom na jej stanovenie. V tomto prípade sa tak uplatní výnimka z uvedeného zákazu spracúvania osobných údajov osobitnej kategórie v zmysle čl. 9 ods. 1 nariadenia. Takáto formulácia povinnosti zamestnávateľa však musí byť pomerne konkrétna čo do svojho obsahu, t. j. spolu s takouto povinnosťou zamestnávateľa je nevyhnutné zabezpečiť „primeranú“ ochranu tohto osobného údaju osobitnej kategórie v podobe prijatia potrebných bezpečnostných opatrení, aby neprišlo k jeho zneužitiu a uplatnila sa bezprostredná ochrana oprávnených záujmov a základných práv dotknutých osôb (zamestnancov odborovo organizovaných).

5.5 Možnosti zvýšenia pracovnoprávnej ochrany zamestnancov prostredníctvom kolektívnej zmluvy

Všeobecné nariadenie o ochrane údajov v porovnaní s pôvodným právnym stavom zavádza v recitáli č. 155 a následne aj v čl. 9 ods. 2 písm. b) posilnenie princípu participácie zástupcov zamestnancov na rozhodovaní a konaní zamestnávateľa v oblasti ochrany osobných údajov. V recitáli č. 155 sa umožňuje v kolektívnych zmluvách (v právnom poriadku Slovenskej republiky v kolektívnych zmluvách vyššieho stupňa), vrátane podnikových kolektívnych zmlúv, stanoviť konkrétne pravidlá upravujúce spracúvanie osobných údajov zamestnancov v súvislosti so zamestnaním, najmä podmienky, za ktorých sa môžu na základe súhlasu zamestnanca spracúvať osobné údaje v súvislosti so zamestnaním na účely prijatia do zamestnania, plnenia pracovnej zmluvy, vrátane plnenia povinností vyplývajúcich z právnych predpisov alebo kolektívnych zmlúv, na účely riadenia, plánovania a organizácie práce, rovnosti a rozmanitosti na pracovisku, ochrany zdravia a bezpečnosti pri práci, ako aj na účely uplatňovania a využívania práv a výhod súvisiacich so zamestnaním na individuálnom alebo kolektívnom základe a na účely ukončenia pracovného pomeru.

V aplikačnej praxi vidíme určite priestor pre výraznejšiu možnosť subjektov pracovnoprávneho vzťahu, osobitne odborových organizácií, aby prostredníctvom kolektívnych zmlúv upravili pravidlá získavania osobných údajov a s odkazom na čl. 9 ods. 2 písm. b) nariadenia aj osobných údajov osobitnej kategórie, a to najmä v oblastiach, kde pracovnoprávna úprava do značnej miery absentuje, resp. je nedostatočná (napr. posudzovanie zdravotnej spôsobilosti zamestnanca na výkon práce a participácia zástupcov zamestnancov v predmetnej oblasti, oblasť predzmluvných vzťahov v zmysle § 41 Zákonníka práce a uzatváranie pracovnoprávnych vzťahov s mladistvými zamestnancami a pod.). V uvedenom prípade možno v zmysle čl. 9 ods. 2 písm. b) nariadenia rovnako stanoviť zamestnávateľovi rozsah ďalších povinností a zamestnancom osobitných práv v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany v rámci kolektívnej zmluvy za predpokladu poskytnutia primeraných záruk ochrany základných práv a záujmov dotknutej osoby, čo by opätovne mohlo viesť k zlepšeniu pracovnoprávnej ochrany zamestnancov v pracovnoprávnych vzťahoch (ako možnosť určitej „pozitívnej diskriminácie“ v pracovnoprávnych vzťahoch v oblasti ochrany osobných údajov).

Právny základ pre úpravu spracúvania osobných údajov v zmysle čl. 9 ods. 2 písm. b) nariadenia však nemožno použiť ako právny základ spracúvania informácie o odborevej príslušnosti zamestnancov pre zamestnávateľa v súvislosti s realizáciou zrážok zo mzdy na účel výberu členského príspevku.

Špecifickým a do budúcnosti pre oblasť vytvorenia nového právneho základu potenciálne najperspektívnejším riešením je prijatie relevantnej právnej úpravy pre posudzovanie dodržiavania zásady rovnakého zaobchádzania a zákazu diskriminácie pri realizácii pracovnoprávnych vzťahov vo väzbe na výkon kompetencií zástupcov zamestnancov (odborovej organizácie) v zmysle § 239 Zákonníka práce. Ustanovenie § 239 Zákonníka

práce umožňuje zástupcom zamestnancom výkon kontroly nad dodržiavaním pracovnoprávnych predpisov, vrátane mzdových predpisov a záväzkov vyplývajúcich z kolektívnej zmluvy. Realizácia výkonu tejto kompetencie však bola s ohľadom na súčasnú právnu úpravu, vrátane jej právnej interpretácie v oblasti ochrany osobných údajov, sťažená, keďže sa mzda zamestnanca považovala za osobný údaj zamestnanca. Vo výsledku tak boli odborovej organizácii, pri snahe o získanie relevantných informácií od zamestnávateľa o prehľade miezd zamestnancov pre možnosť výkonu kontroly v zmysle § 239 Zákonníka práce, poskytnuté výlučne štrukturované údaje za kategóriu zamestnancov bez ich personalizácie vo vzťahu k jednotlivým zamestnancom. Hoci predmetné údaje postačovali na objektívny výkon kontroly zvýšenia napr. priemerného zárobku zamestnancov za celú skupinu, nebolo možné na ich podklade posúdiť práve spomínané konkretizované “rovnaké” zaobchádzanie so zamestnancami z dôvodu, že nebolo možné identifikovať vhodného komparátora pre porovnanie.

Pri posudzovaní rovnakého zaobchádzania so zamestnancami (dodržanie zákazu diskriminácie v zmysle čl. 1 Základných zásad Zákonníka práce vo väzbe na § 13 Zákonníka práce) sa totiž vyžaduje pre možnosť ďalšieho postupu zo strany odborovej organizácie, aby si dokázala predbežne vyhodnotiť skutkový i právny stav z pohľadu, či prišlo (prichádza) k nerovnakému zaobchádzaniu so zamestnancom alebo k jeho diskriminácii. Napriek skutočnosti, že právo Európskej únie a vo väzbe na neho i antidiskriminačný zákon formulujú dôkazný procesný postup spôsobom, že dôkazné bremeno spočíva na žalovanom (zamestnávateľovi), v aplikačnej praxi sa postup trochu líši. Za predpokladu, že sa zamestnanec so svojou sťažnosťou v zmysle § 13 ods. 5 Zákonníka práce obráti na zamestnávateľa, spravidla sa súčasne domáha ochrany svojich práv a oprávnených záujmov aj u odborovej organizácie v zmysle § 232 ods. 2 alebo ods. 3 Zákonníka práce. Posudzovanie prípadu sa spravidla odvíja súčasne dvomi procesnými spôsobmi, keď pre vybavovanie sťažností zamestnancov sú v spoločnostiach, kde pôsobia zástupcovia zamestnancov, komisie zriadené na bipartitnom princípe. Popri posudzovaní prípadu v rámci komisií súčasne vykonáva vlastné vyšetrenie sťažnosti aj odborová organizácia, pričom na tento účel požaduje od zamestnávateľa poskytnutie konkrétnych personalizovaných informácií. Musíme totiž upozorniť na skutočnosť, že zväčša sa dominantná časť týchto prípadov, kedy sa zamestnanec domáha ochrany pri porušení zásady rovnakého zaobchádzania alebo porušení zásady zákazu diskriminácie, dotýka odmeňovania zamestnancov. Jeden alebo viacerí zo skupiny zamestnancov sú lepšie odmeňovaní ako ostatní, otázkou zostáva, či je odlišné odmeňovanie založené na subjektívnom princípe (ktorý z nášho pohľadu môže zakladať domnienku nerovnakého zaobchádzania) alebo na objektívnom princípe (v zmysle čl. 1 Základných zásad Zákonníka práce) a či môže byť rozdielne zaobchádzanie odôvodnené povahou činností vykonávaných v zamestnaní alebo okolnosťami, za ktorých sa tieto činnosti vykonávajú, ak tento dôvod tvorí skutočnú a rozhodujúcu požiadavku na zamestnanie pod podmienkou, že cieľ je legitímny a požiadavka primeraná. K rozlíšeniu subjektívnych a objektívnych dôvodov odlišného zaobchádzania musí však súčasne pristúpiť ďalšia

právetvorná skutočnosť, t. j. že pri komparácii zamestnancov budeme využívať vhodných komparátorov (porovnateľnosť zamestnancov z pohľadu vykonávanej pracovnej pozície, dĺžky trvania pracovného pomeru, pokiaľ môže byť odlišné odmeňovanie založené na princípe seniority, rozsahu pracovných úloh a pod.).

Hoci tak môže odborová organizácia na podklade vlastnej činnosti určiť vhodného komparátora (porovnateľného zamestnanca), nemusí disponovať poznatkami o výške a štruktúre jeho mzdy, pričom štrukturované informácie, poskytnuté v zmysle § 239 Zákonníka práce, takúto informáciu neobsahujú. Následne preto odmietnutie poskytnutia informácie o výške a štruktúre mzdy porovnateľného zamestnanca s odôvodnením, že ide o osobný údaj zamestnanca môže de facto zmariť možnosť zamestnanca domáhať sa ochrany svojich práv pri podozrení na porušenie zásady rovnakého zaobchádzania v pracovnoprávných vzťahoch.

Vhodným riešením sa preto javí per analogiam s odkazom na čl. 9 ods. 2 písm. b) všeobecného nariadenia na ochranu údajov využitie predmetnej výnimky a stanovenie nových pravidiel pre spracúvanie ochrany osobných údajov spôsobom, ktorý by vo vybraných prípadoch umožnil odborovej organizácii dožadovať sa predmetných osobných údajov, vrátane osobitných kategórií osobných údajov, pričom zamestnávateľ by bol povinný takéto údaje poskytnúť v zmysle záväzku formulovaného v kolektívnej zmluve. Neuplatnenie zákazu spracúvania osobitných kategórií osobných údajov, a tým aj nemožnosť zamestnávateľa odvolávať sa na ich ochranu a nemožnosť ich poskytnutia tretej osobe, by bolo odôvodnené práve uvádzanou výnimkou. Formulácia takéhoto záväzku by si však pochopiteľne vyžadovala poskytnutie priemeraných záruk ochrany základných práv a záujmov dotknutej osoby (zamestnanca považovaného za vhodného komparátora):

- presné označenie prípadov, v ktorých sa bude predmetná výnimka uplatňovať,
- rozsah a štruktúra poskytovaných informácií a forma ich spracúvania,
- doba spracúvania týchto osobných údajov,
- forma a prostriedky ich zabezpečenia pred nepovoleným prístupom tretej strany a pod.

Záver

Zohľadnenie novej právnej úpravy v oblasti ochrany osobných údajov do aplikačnej praxe pri realizácii individuálnych a kolektívnych pracovnoprávných vzťahov si bude vyžadovať dôkladné posúdenie všetkých relevantných súvislostí, predovšetkým vo väzbe na ich procesnoprávnu stránku. Nové nakladanie s rodným číslom alebo fotografiou zamestnanca, problematika whistleblowingu či monitorovania zamestnancov prostredníctvom rôznych telekomunikačných a audiovizuálnych prostriedkov predstavujú ťažiskové prípady, v rámci ktorých bude musieť prísť k novému nastaveniu vzťahov medzi subjektmi pracovnoprávných vzťahov.

Obdobne však vyvstanú nové povinnosti, ale aj príležitosti pre zamestnávateľa i zástupcov zamestnancov, v oblasti kolektívneho vyjednávania a najmä obsahu kolektívnej zmluvy, keď zmluvným stranám vznikne možnosť zaviesť relevantnú právnu úpravu v podobe nového právneho základu pre spracúvanie osobných údajov, napr. v predzmluvných vzťahoch alebo zaviesť nové primerané (bezpečnejšie) záruky pre zamestnancov i zamestnávateľa pri uplatňovaní jednotlivých pracovnoprávných inštitútov, v rámci ktorých prichádza k získavaniu osobných údajov dotknutých osôb.

Nová právna úprava tak so sebou prináša zásadné výzvy pre oblasť pracovného práva, z ktorých následne môžu vyjsť víťazi, ale aj porazení a bude závisieť na samotných sociálnych partneroch, či takúto situáciu pripustia, alebo sa budú snažiť dosiahnuť obojstranne výhodné dohody.

Základným predpokladom pre úspech však bude dostatočné si osvojenie novej problematiky, a to nielen z pohľadu samotného zamestnávateľa, ale najmä zástupcov zamestnancov i zamestnancov.

Predkladaná publikácia má ambíciu stať sa základným východiskom pre štúdium novej právnej úpravy v oblasti ochrany osobných údajov a jej dopadov do oblasti pracovnoprávných vzťahov a prostredníctvom jednotlivých prípadových štúdií prispieť k odpovedajúcemu si osvojeniu celej matérie nielen odbornou, ale i laickou verejnosťou.

Zoznam použitej literatúry

- BARANCOVÁ, H. 2010. *Monitorovanie zamestnancov a právo na súkromný život*. Bratislava: Sprint dva, 2010.
- BARANCOVÁ, H. 2016. Nové technológie v pracovnom práve a ochrana zamestnanca (možnosti a riziká). Praha: Leges, 2016, s. 25 a nasl.
- BARANCOVÁ, H. a kol. 2017. *Zákonník práce. Veľký komentár*. Praha: C.H.Beck, 2017.
- BARINKOVÁ, M. 2015. Bezúhonnosť zamestnanca. In *Personálny a mzdový poradca podnikateľa*. ISSN 1335-1508. Roč. 21, č. 9-10 (2015), s. 42-54.
- BARINKOVÁ, M. – SEILEROVÁ, M. 2016. *Ochrana oznamovateľov protispoločenskej činnosti*. In: *Súčasný stav a nové úlohy pracovného práva: Dies Iuris Tyrnaviensis-Trnavské právnické dni: Nová Európa-výzva a očakávania: medzinárodná vedecká konferencia: 22.-23.9.2016, Trnava*. Praha: Nakladatelství Leges, 2016, s. 83-98.
- BARINKOVÁ, M. – VARGA, V. – SOKOL, P. 2017. Vplyv elektronizácie na formy oznamovania protispoločenskej činnosti. In: *Právo, obchod, ekonomika VII.: zborník príspevkov z vedeckého sympózia: 11. - 13. október 2017, Vysoké Tatry*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2017, s.177-192.
- BÖHMOVÁ, L. – PAVLÍČEK, A. 2013. Personalistika a budúcnosť sociálnych sítí v ČR; in: *Scientific Papers of the University of Pardubice. Series D, Faculty of Economics & Administration*, 2013, roč. 20, č. 27, s. 14 – 22.
- BULLA, M. 2010. Ochrana súkromia zamestnancov optikou judikatúry Súdneho dvora Európskej únie. In: *Monitorovanie zamestnancov a právo na súkromný život*. Bratislava : Sprint dva, 2010, s. 69–82.
- ČAPEK, J. 1995. *Evropský soud a Evropská komise pro lidská práva*. Praha : Linde Praha a.s., 1995.
- DENNIS, C. M. 2011. *Legal implications of employee social media use*. In *Massachusetts Law Review*, 2011, Vol. 93. Number 4. s. 380–395.
- DOLOBÁČ, M. 2016. Kontrola elektronických komunikačných prostriedkov v pracovnoprávných vzťahoch. In *Právo, obchod, ekonomika VI.: zborník príspevkov z vedeckej konferencie: 26. - 28. októbra 2016, Vysoké Tatry*. - Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2016, s. 145-152.
- DOLOBÁČ, M. 2015. Kvóta systém v pracovnom práve. In: *Diskriminácia v zmluvnom práve: 3. december 2014, Trnava*. Bratislava: Typi Universitatis Tyrnaviensis, 2015, s. 111-120.
- DOLOBÁČ, M. 2010. Monitoring e-mailovej komunikácie zamestnanca v judikatúre Európskeho súdu pre ľudské práva. In: *Monitorovanie zamestnancov a právo na súkromný život: zborník vedeckých príspevkov*. Bratislava: Sprint dva, 2010, s. 118-126.

- HRUŠOVSKÁ, V. – OLŠOVSKÁ, A. 2013. Whistleblowing na pracovisku – právna úprava, teória a prax na Slovensku. In *Whistleblowing*. Praha : Wolters Kluwer CR, 2013, s. 127 – 143.
- KNAP, K. – ŠVESTKA, J. – JEHLÍČKA, O. – PAVLÍK, P. – PLECITÝ, V. 2004. *Ochrana osobnosti podle občanského práva*. 4. podstatně prepracované a doplněné vyd.. Praha : Linde, 2004.
- KOVÁČ, P. *Zrušenie rodného čísla – drahá a zbytočná sranda*. Dostupné na internete: <https://dennikn.sk/blog/zrusenie-rodneho-cisla-draha-a-zbytocna-sranda/>.
- LAZAR, J. a kol. 2006. *Občianske právo hmotné*. Bratislava : Iura Edition, 2006.
- LUKIČ, L. – SOKOL, P. 2014. *(Ne)bezpečie sociálnych sietí*. prvé vydanie, vydalo European Information Society Institute, o. z., v roku 2014, s. 9, ISBN 978-80-971307-2-5. Dostupné na:
 - http://www.eisionline.org/files/nebezpecenstvo_socialnych%20sieti.pdf
- MADLEŇÁK, A. Integrácia reálneho a virtuálneho sveta prostredníctvom QR kódov = The integration of virtual and real world using QR codes. In: *Manažment environmentálnych inovácií prostredníctvom phygitalových nástrojov*. editori: Anna Zaušková, Adam Madleňák; recenzenti: Jana Štofková, Andrea Sujová. - 1. vyd. - Trnava : Univerzita sv. Cyrila a Metoda v Trnave, Fakulta masmediálnej komunikácie, 2017. - ISBN 978-80-8105-900-1, S. 63-71.
- MADLEŇÁK, A. - RADOŠINKSKÁ, J. AIDC in the digital world or how to identify data via GTIN codes in retails and small enterprises. In: *Marketing Identity : Digital Life - part II. : Conference Proceedings from International Scientific Conference 10th - 11th November 2015, Congress Hall of the Slovak Academy of Sciences, Smolenice, Slovak Republic* / editors: Jozef Matúš, Dana Petranová. - 1. vyd. - Trnava : Faculty of Mass Media Communication, University of Ss. Cyril and Methodius in Trnava, 2015. - ISBN 978-80-8105-780-9. - ISSN 1339-5726, S. 139-147.
- MATEJKA, J. 2013. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha : CZ.NIC, 2013.
- MERRELL, L. EU General Data Protection Regulation – The impact on employers. Dostupné na internete: http://www.clarkslegal.com/Blog/Post/EU_General_Data_Protection_Regulation_The_impact_on_employers.
- MICHALÍČEK, F. 2014. Právo na súkromie zamestnancov v judikatúre Slovenskej republiky a Českej republiky. In *Societas et Iurisprudentia*, č. 1, 2014, s. 131-146.
- MORÁVEK, J. 2013. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer ČR, 2013.
- MURA, L. – ŽULOVÁ, J. – MADLEŇÁK, A. 2016. Strategic management and management of personnel costs: employing young people in the Slovak Republic. In *Problems and perspectives in management*. roč. 14, č. 1, 2016, s. 79-84.
- ROBERTS, S. – J. – ROACH, T. 2009. Social networking websites and human resource personnel: Suggestions for job searches. In *Business Communication Quar-*

terly, 2009. Volume 72. Issue 1, s. 110–114.

- SISKOVÍČOVÁ, K. 2015. *Ochrana súkromia a osobných údajov zamestnanca*. Trnava: Vydavateľstvo Typi Universitatis Tyrnaviensis, 2015.
- ŠTEFKO, M. 2005. Kproblému sledování vlastních zaměstnanců. In *Právo a zaměstnání* č. 1, 2005, s. 7-11.
- ŠVEC, M., VALENTOVÁ, T. *Ochrana osobných údajov v pracovnoprávných vzťahoch*. Bratislava: Wolters Kluwer, 2016, s.38.
- TOMAN, J. 2014. *Individuálne pracovné právo. Všeobecné ustanovenia a pracovná zmluva*. Bratislava: Friedrich Ebert Stiftung, zastúpenie v SR, 2014.
- VARGA, P. Ochrana osobnosti v kontexte historického výskumu. In *Genealogicko-heraldický hlas*, roč. 26, č. 1, s. 79 – 85.
- VOJTKO, Jakub. 2017. Automatizované rozhodovanie a profilovanie v pracovnoprávných vzťahoch podľa Všeobecného nariadenia o ochrane údajov. In *Časopis pro právní vědu a praxi*. [Online]. 2017, č. 2, s. 255-274. [cit. 2017-11-14]. Dostupné z: <https://journals.muni.cz/cpvp/article/view/6322>.
- ZIMEN, O. Autentifikácia rodným číslom – áno alebo nie? Dostupné na internete: <https://www.pravnenoviny.sk/spravne-pravo/autentifikacia-rodnym-cislom-ano-alebo-nie>.
- ŽULOVÁ, J. 2016. Chcete zmeniť zdravotnú poisťovňu? In: *Práce a Mzdy bez chýb, pokút a penále*. Roč. XI. č. 7-8 (2016), s. 3-4.
- ŽULOVÁ, J. 2016. Používanie sociálnych sietí pri výbere zamestnancov (z pracovnoprávneho hľadiska). In *Justičná revue*, 68, 2016, č. 6-7, s. 729 – 736.

GDPR A OCHRANA ZÁUJMOV ZAMESTNANCA

Autorský kolektív: JUDr. Jana Žuřová, PhD.,
doc. JUDr. Marek Švec, PhD., LL.M.
Recenzenti: doc. JUDr. Mgr. Andrea Olšovská, PhD.
JUDr. Marcel Dolobáč, PhD.
JUDr. Simona Schuszteková, PhD., LL.M.
Vydavateľ: Friedrich Ebert Stiftung, zastúpenie v SR; Bratislava 2018
Návrh obálky: Mgr. Jakub Filo
Rok a miesto vydania: Bratislava, 2018
Rozsah publikácie: 10,4 AH

Vychádza v tlačennom náklade 300 ks.

Právne výklady a stanoviská obsiahnuté v texte publikácie sú subjektívnym názorom autorského kolektívu, nemožno ich stotožňovať s postojmi Friedrich Ebert Stiftung, e.V. alebo Labour Law Association/Asociácia pracovného práva. Toto dielo a ani žiadnu jeho časť nemožno reprodukovat' bez súhlasu Friedrich Ebert Stiftung, e.V..

ISBN 978-80-89149-57-5 (tlačený - lepený/mäkká väzba)

Nový právny rámec ochrany osobných údajov tvorený európskym všeobecným všeobecným nariadením o ochrane údajov a novým slovenským zákonom o ochrane osobných údajov predstavuje pre mnoho dotknutých osôb, ktoré by sa ním mali riadiť, nanešťastie stále pomerne veľkú neznámu.

V nadväznosti na opakované požiadavky i dotazy z aplikačnej praxe sa preto autorský kolektív rozhodol aj s ohľadom na vlastné profesionálne zameranie i predchádzajúce teoretické i praktické skúsenosti s ochranou osobných údajov v súčasnom právnom rámci pripraviť predkladanú publikáciu dotýkajúcu sa identifikácie zmien, ktoré si vyžiada pri realizácii pracovnoprávných vzťahov uplatnenie nového všeobecného nariadenia o ochrane údajov.

Postupným predmetom výkladu sa stáva nielen otázka práva na súkromie ako základného imperatívu ochrany osobných údajov, ale aj otázky súvisiace vôbec s vymedzením okruhu dotknutých subjektov, konkretizácie ich práv a povinností alebo upresnenia nových právnych inštitútov, ktoré so sebou nová právna úprava prináša. Základnou pridanou hodnotou publikácie je uvedenie prípadových štúdií, ktoré umožňujú čitateľovi osvojiť si náročnú problematiku prostredníctvom riešenia konkrétnych problémov, s ktorými sa stretáva najčastejšie vo svojej praxi.

ISBN 978-80-89149-57-5



9 788089 149575 >



LABOUR LAW ASSOCIATION
ASOCIÁCIA PRACOVNÉHO PRÁVA

FRIEDRICH
EBERT
STIFTUNG