UNIVERZITA KARLOVA
Právnická fakulta

Mgr. Matěj Tkadlec

Ochrana osobních údajů podle GDPR se zaměřením na pracovněprávní vztahy a biometriku

Rigorózní práce

Pověřený akademický pracovník: doc. JUDr. Jakub Morávek, Ph.D.

Tématický okruh: Pracovní právo

Datum vypracování práce (uzavření rukopisu): 9. ledna 2022

Prohlašuji, že jsem předkládanou rigorózní práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 257.846 znaků včetně mezer.

Mgr. Matěj Tkadlec

V Praze dne 9. ledna 2022

Poděkování

Tímto bych chtěl velmi poděkovat svému školiteli, panu doc. JUDr. Jakubu Morávkovi, Ph.D., za všechny jeho cenné rady a za jeho vedení nejen při psaní této rigorózní práce, ale i v průběhu mých dalších studií. Jeho času i podpory, kterou mi věnuje, si velmi vážím.

OBSAH

1. Úvod

Je to již více než tři roky, kdy vešlo v platnost nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,[1] o kterém bude v této práci dále referováno již pouze jako o Nařízení. K dnešnímu dni je to tedy více než pět let od momentu, kdy se nad celkovým zněním Nařízení a jeho skutečnými dopady začaly vést bohaté akademické diskuze i mimo legislativní proces Evropské unie. Vzhledem k tomuto časovému rámci je přitom nasnadě zamyslet se hlouběji nad tím, zda Nařízení ve své obecnosti lze označit spíše za pozitivní, či spíše negativní legislativní počin evropského zákonodárce a zda jsou právní procesy a instituty Nařízení již dnes správně chápané a bez větších obtíží aplikované.

Tato rigorózní práce si přitom klade za cíl věnovat se Nařízení a hodnotit jeho dopad především v oblasti pracovněprávních vztahů jako poměrně svébytného a specifického sektoru ochrany osobních údajů. Že vztahy mezi zaměstnavateli a zaměstnanci jsou z hlediska ochrany osobních údajů atypickou formou regulace přitom plyne již z recitálu (155) Nařízení, který uvádí, že: *„Právo členského státu nebo kolektivní smlouvy (včetně „podnikových dohod“) mohou stanovit zvláštní pravidla, která upraví zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména podmínky, za nichž lze osobní údaje v souvislosti se zaměstnáním zpracovávat na základě souhlasu zaměstnance, za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a různorodosti na pracovišti, zdraví a bezpečnosti na pracovišti, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.“* Jak vidno, ochrana osobních údajů v pracovněprávních vztazích má několik časových pásem, ve kterých zaměstnavatel osobní údaje svých zaměstnanců zpracovává, resp. ve kterých

[1] Jak název Nařízení napovídá, v důsledku jeho přijetí došlo ke zrušení Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Nařízení bylo schváleno dne 27. dubna 2016, přičemž mělo stanovenou nebývale dlouhou legisvakanční lhůtu, neboť účinnosti nabylo až 25. května 2018. I když Nařízení nezměnilo ve srovnání se Směrnicí základní teleologické ani principiální východiska ochrany osobních údajů, a ani významným způsobem nerozšiřovalo působnost, evropský zákonodárce jeho přijetím za prvé zvýšil nároky na ochranu osobních údajů a za druhé významně unifikoval velmi svébytnou a významnou právní oblast. Před Nařízením přitom neexistoval jiný institut práva EU, který by tak významným způsobem zasáhl do právních řádů všech členských států a legiskvanční lhůtu v délce 2 let tak lze označit za krok dobrým směrem.

mezi ním a jeho zaměstnanci vznikají na úseku ochrany osobních údajů právní vztahy. Jedná se o:

(i) zpracování osobních údajů ještě před vznikem pracovního poměru, tedy v rámci výběrového řízení;

(ii) zpracování osobních údajů v průběhu pracovněprávního vztahu; a

(iii) specifika nakládání s nimi při, resp. po skončení pracovněprávního vztahu.[2]

Nicméně předtím, než se tato práce soustředí na specifickou povahu pracovněprávních vztahů, zaměří se na obecnější rovinu práva na ochranu osobních údajů.

V první řadě bude proveden právní rozbor některých významných pojmů, jež se na úseku ochrany osobních údajů obecně vyskytují a které je potřeba si nejdříve pomocí současné doktríny a judikatury vymezit tak, aby bylo možno s nimi nadále v této stati pracovat v jejich správném slova smyslu. V dalším se práce zaměří zejména na podrobné zkoumání povinností, které na základě Nařízení vznikají na straně správců a zpracovatelů osobních údajů, a na to, jak se tyto projevují především právě v pracovněprávních vztazích. V návaznosti na tuto pasáž bude v další části práce věnována pozornost samozřejmě i právům a oprávněným zájmům subjektu údajů, tedy těch osob, jejichž osobní údaje jsou ze strany správců zpracovávány.

Po takto zpracované obecné části se práce zaměří na konkrétní problémy ochrany osobních údajů zaměstnanců. V této pasáži však nebude problematika ochrany osobních údajů zpracovávána pouze z pohledu Nařízení, ale také z pohledu českého zákoníku práce, tedy zákona č. 262/2006 Sb., relativně nového zákona č. 110/2019 Sb., o zpracování osobních údajů, zákona č. 198/2000 Sb., antidiskriminační zákon a také z pohledu zákonných norem ústavního práva a dalších evropsko-právních předpisů.[3] Při jakémkoli odborném zpracování problematiky ochrany osobních údajů, bez ohledu na to, zda v pracovněprávních či jakýchkoli jiných vztazích, nelze totiž opomenout skutečnost, že tato velmi úzce souvisí s otázkou soukromí jedince jako lidskoprávní maximy. V poslední části pak bude věnována pozornost zejména

[2] Jak totiž vyplývá z uvedeného recitálu, mohou být stanovena zvláštní pravidla pro zpracování (i) za účelem náboru, (ii) plnění pracovní smlouvy a (iii) ukončení zaměstnaneckého poměru.

[3] Z hlediska ústavněprávního lze zmínit kupříkladu úpravu práva na soukromí uvedenou v čl. 7 Listiny základních práv a svobod. Z hlediska evropsko-právního například Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, které je podstatným institutem zejména s ohledem na elektronizaci pracovněprávních spisů a obecně využívání moderních technologií evidence dokumentace a elektronických podpisů.

oblasti biometrických údajů jako zvláštní kategorie osobních údajů dle Nařízení,[4] využívání moderních technologických prostředků při elektronizaci pracovněprávní dokumentace a na limity, ve kterých se zaměstnavatel musí při praktickém užití uvedených institutů pohybovat.

Cílem této práce nebude pojednat o každém jednotlivém problematickém aspektu ochrany osobních údajů v pracovněprávních vztazích v jeho úplné celistvosti, neboť to vzhledem k jejímu rozsahu ani není možné. Práce si nicméně klade za cíl po zevrubném popisu základních institutů, povinností správců a zpracovatelů a práv subjektu údajů za užití deskriptivní výzkumné metody kriticky zhodnotit a analyticky popsat funkčnost některých technologických prostředků zpracování s důrazem na biometrické údaje, a to vše perspektivou pracovněprávních vztahů.

[4] Co se rozumí zvláštní kategorií osobních údajů (citlivé osobní údaje), je uvedeno například v recitálu (53) Nařízení, přičemž rozhodující ve vztahu k jejich zpracování je čl. 9 Nařízení.

2. Základní definiční pojmy dle Nařízení

Za účelem dalšího zkoumání jednotlivých aspektů ochrany osobních údajů v pracovněprávních vztazích, zejména jejich správné analýzy, identifikaci jejich nejproblematičtějších úskalí a ve snaze nastínit, jak by k nim mělo být přistupováno v praxi, je potřeba v této práci prvně vymezit základní pojmy systému ochrany osobních údajů. Právní regulace ochrany osobních údajů totiž obsahuje mnoho zvláštních definic, které se v čase vyvíjí, a které je pro správné pochopení potřeba blíže prozkoumat.[5]

2.1. Osobní údaj

Nejzákladnějším pojmem celého systému ochrany osobních údajů je osobní údaj. Nařízení osobní údaje definuje, jako: *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*.[6] Pokud se blíže neurčeného pojmu informace o identifikovatelné podobě týče, je v této souvislosti dále rovněž podstatný recitál (26) Nařízení, kde je uvedeno, že: *„Zásady ochrany údajů by se měly uplatňovat na všechny informace týkající se identifikované nebo identifikovatelné fyzické osoby. Osobní údaje, na něž byla uplatněna pseudonymizace a jež by mohly být přiřazeny fyzické osobě na základě dodatečných informací, by měly být považovány za informace o identifikovatelné fyzické osobě* (a tedy za osobní údaje – pozn. autora). *Při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji. Zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není*

[5] Většina pojmů, které budou blíže popsány v této kapitole, jsou definovány buďto již v samotné preambuli Nařízení, nebo jejich definici obsahuje čl. 4 Nařízení.
[6] Srov. čl. 4 odst. 1 Nařízení.

nebo již přestal být identifikovatelným. Toto nařízení se tedy netýká zpracování těchto anonymních informací, včetně zpracování pro statistické nebo výzkumné účely.“

Ještě před přijetím Nařízení, když byla ochrana osobních údajů v evropském měřítku normována směrnicí o ochraně fyzických osob v souvislosti se zpracováním osobních údajů,[7] která tvořila referenční rámec v oblasti ochrany osobních údajů v Evropské unii, bylo pracovní skupinou WP 29[8] vydáno k pojmu osobní údaj stanovisko č. 4/2007.[9] Toto stanovisko je bez pochyby použitelné i dnes, neboť ve Směrnici byl osobní údaj definován *de facto* stejným způsobem, jakým je definován v Nařízení, a sice *„Osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.“* Stanovisko přitom právě s touto definicí Směrnice pracovalo. Na jejím základě pracovní skupina WP 29 dospěla k závěru, že se uvedená definice sestává ze čtyř hlavních složek, kterými jsou:

(i) veškeré informace;

(ii) „o“ (vztah mezi informacemi a osobou);

(iii) identifikovaná nebo identifikovatelná; a

(iv) fyzická osoba.

Pojem veškeré informace byl již ve světle Směrnice vykládán velmi extenzivně a s ohledem na výše citovaný recitál (26) tomu nebude jinak ani za účinnosti Nařízení. Těmito informacemi je třeba rozumět všechny informace o určitém jedinci, ať už objektivní (přítomnost určité látky v krvi), či subjektivní (názory a přesvědčení) povahy, bez ohledu na to, zda se jedná o informace pravdivé či prokazatelné, a bez ohledu na jejich obsahovou povahu (tedy nehledě na skutečnost, čeho se daná informace o konkrétním jedinci týká). Důvodem, proč se ochrana osobních údajů vztahuje na tak široké penzum informací, je především úzké spojení této právní oblasti s ochranou soukromí a ochranou osobnosti každého jedince, jíž je v celoevropském

[7] Celým názvem Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
[8] Skupina WP 29 byla zřízena na základě čl. 29 Směrnice v roce 1996 a jednalo se o poradní orgán ve věci ochrany osobních údajů tvořený orgány zodpovědnými za ochranu osobních údajů každého členského státu EU. V květnu 2018 tedy společně s účinností Nařízení byla nahrazena Evropským sborem pro ochranu osobních údajů.
[9] Stanovisko pracovní skupiny WP 29 z 20. července 2007, č. 4/2007 (WP 136).

měřítku poskytována velmi široká ochrana.[10] Uvedené plyne např. i z judikatury jak tuzemských soudů, tak např. SDEU, ze které je patrné, že pojem osobní údaj je skutečně vnímán velmi extenzivně.[11]

Stejně tak není dle stanoviska č. 4/2007 skupiny WP 29 rozhodný formát informací a nosič, který je obsahuje. Dále se stanovisko speciálně zmiňuje také o biometrických údajích, kterým bude v této rigorózní práci věnována speciální pozornost, když uvádí: *„Tyto údaje lze definovat jako biologické vlastnosti, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti. K typickým příkladům biometrických údajů patří otisky prstů, struktura sítnice, struktura obličeje či hlas, ale také geometrie ruky, struktura žil, nebo dokonce některé hluboce zakořeněné dovednosti či jiné behaviorální rysy (například vlastnoruční podpis, úhozy na klávesnici, charakteristický způsob chůze nebo řeči atd.).“*

Druhým kritériem osobního údaje je jeho provázanost k dané osobě, tj. skutečnost, že se předmětná informace týká konkrétní fyzické osoby, tj. je „o“ ní. K posouzení, zda určitá informace je zpracována o některém jedinci, slouží prvky jejího obsahu, účelu a výsledku. Prvek obsahu je pochopitelně přítomný tam, kde již samotná evidence informací obsahuje zjevně primárně údaje o fyzických osobách. Prvek účelu je naplněn tam, kde jsou informace a osobní údaje shromažďovány proto, aby bylo možno nějakou osobu hodnotit, identifikovat či do budoucna s informacemi o ní jinak zacházet. Prvek výsledku funguje jako jakési *ultima ratio*, kdy obsahem *a priori* nejsou informace o určité osobě a účelem jejich zpracování ani nebylo tuto osobu identifikovat, ale prostě se tak v daném případě stane (například poskytnutí informací o vozidle do registru vozidel, pomocí kterých půjde ale identifikovat i vlastníka vozidla).

Rovněž třetí kritérium hlavních složek pojmu osobní údaj, tedy identifikace či identifikovatelnost osoby, musí být a je vykládáno co možná nejextenzivnějším způsobem. Subjekt údajů totiž nemusí být identifikován pouze jménem a příjmením, datem narození, rodným číslem či adresou (tedy skrze identifikaci přímou), ale také prostřednictvím jedinečných

[10] Srov. například rozsudek Evropského soudu pro lidská práva ve věci Amann v. Švýcarsko ze dne 16. února 2000, č. 22298/95 či rozsudek téhož soudu ve věci Niemietz v. Německo ze dne 16. prosince 1992, č. 13710/88.
[11] Srov. např. rozhodnutí SDEU ze dne 6. listopadu 2003, sp. zn. C-101/01, ve věci Bodil Lindqvist (pracovní úraz) či rozhodnutí SDEU ze dne 20. října 2016, sp. zn. C-582/14, ve věci Patrick Breyer vs. Bundesrepublik Deutschland (IP adresa) nebo také rozhodnutí NSS ze dne 12. února 2009, sp. zn. 9 As 34/2008 (telefonní číslo).

kombinací specifických identifikátorů, které v důsledku vzájemného propojení mohou danou osobu identifikovat nepřímo.

V případě osobních údajů vedoucích k nepřímé identifikaci či identifikovatelnosti přitom záleží na posouzení, jak moc jsou tyto nepřímé informace specifické v rámci určitého okruhu zatím neznámých osob. Tak například informace o tom, že se na pracovní pozici přihlásila žena, která momentálně vykonává funkci ústavní soudkyně, může jistě být osobním údajem ve smyslu výše uvedeného již sama o sobě, neboť momentálně má český Ústavní soud pouze dvě soudkyně. Pokud však informace bude znít tak, že se na pracovní pozici přihlásila žena, která momentálně vykonává funkci soudkyně, ani na základě nepřímého určení nebude taková informace osobním údajem, neboť jen pomocí ní nelze identifikovat ani užší okruh osob, ke kterému by se mohla vztahovat.

Zda tedy daná informace je s to identifikovat určitou konkrétní osobu, je vždy nutno poměřovat *ad hoc* s přihlédnutím ke všem významným okolnostem daného případu. K tomu blíže také například judikatura Nejvyššího správního soudu, kde se k pojmu osobní údaj, identifikovatelnosti a rozlišení identifikace přímé a nepřímé uvádí, že: *„V intencích výše uvedeného lze tak obecně fyzickou osobu považovat za „identifikovanou“, jestliže je ve skupině osob odlišena ode všech ostatních příslušníků této skupiny. V souladu s tím je fyzická osoba „identifikovatelná“, jestliže je možné ji identifikovat (přípona „-elná“ vyjadřuje možnost), ačkoli dosud identifikována nebyla. Tato druhá alternativa proto v praxi představuje prahovou podmínku určující, zda informace vyhovuje definici osobního údaje.“*[12] či: *„Přímo může být identifikována osoba zpravidla jménem, nepřímo např. podle telefonního čísla, registračního čísla automobilu, čísla sociálního pojištění, čísla cestovního pasu, apod. Nepřímou identifikaci lze provést rovněž pomocí kombinace významných kritérií, která ji umožňují rozeznat zúžením skupiny, do které patří (věk, povolání, bydliště atd.). Z uvedeného vyplývá, že míra dostatečnosti určitých identifikátorů z hlediska provedení identifikace závisí na souvislostech konkrétní situace. Např. běžné příjmení nepostačí k identifikaci – tj. jednoznačnému určení – osoby v celé populaci země nebo ve velkém městě, ale pravděpodobně bude stačit např. k identifikaci studenta ve třídě nebo ubytovaného hosta v hotelu nebo účastníka konkrétního semináře konaného v daném čase v daném místě. (…)“*[13]

[12] Rozhodnutí Nejvyššího správního soudu z 28. června 2013, č. j. 5 As 1/2011-156.
[13] Rozhodnutí Nejvyššího správního soudu z 27. února 2014, č. j. 4 As 132/2013-25.

Kromě uvedeného rozhodnutí lze zmínit také i další rozhodnutí NSS, která se věnovala negativnímu vymezení pojmu osobního údaje a ze kterých např. plyne, že se nejedná o osobní údaj subjektu údajů v případě, když je nutno k identifikaci tohoto subjektu údajů vynaložit nepřiměřené úsilí, resp. když daný údaj v podstatě nelze ztotožnit s konkrétní osobou[14] nebo když je na základě daného údaje identifikovatelnost osoby nemožná nebo pouze zanedbatelná.[15]

2.2. Zvláštní kategorie osobních údajů – citlivé údaje

Některé osobní údaje se těší již z mandatorních ustanovení Nařízení, ale i vnitrostátních právních předpisů jako například ZOZOÚ vyššího stupně ochrany než osobní údaje jiné. Těmito údaji jsou tzv. citlivé údaje (terminologií ZOZOÚ či například recitálu (10) Nařízení) neboli zvláštní kategorie osobních údajů (terminologií Nařízení v těle jeho normativní části).

Nařízení pojem zvláštní kategorie osobních údajů definuje v čl. 9 odst. 1, podle kterého se jimi rozumí údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.[16] Vedle toho Nařízení ještě ve svém definičním článku obsahuje speciální definici pro genetický údaj: „*osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby*“, biometrický údaj: „*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje*“ a pro údaj o zdravotním stavu: *„osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.“*[17]

Tyto jednotlivé subtypy zvláštní kategorie osobních údajů jsou také stěžejní pro bližší pochopení jejich podstaty, neboť například česká odborná komentářová literatura věnuje pozornost všem těmto jednotlivým subtypům, ale pojmu „zvláštní kategorie osobních údajů“

[14] Rozhodnutí NSS ze dne 25. února 2015, sp. zn. 1 As 113/2012.
[15] Rozhodnutí NSS ze dne 20. prosince 2018, sp. zn. 6 As 168/2018.
[16] ZOZOÚ upravuje pojem citlivý údaj pouze v přechodných ustanoveních v § 66, a to za účelem definice tohoto pojmu ve světle dosavadních právních předpisů.
[17] Článek 4 odst. 13, 14 a 15 Nařízení. Z recitálů Nařízení je pak ve vztahu k těmto druhům údajů důležitý recitál (10), recitál (34), recitál (35) a recitál (52), které se k nim vyjadřují ve větší podrobnosti.

jako takovému se v podstatě nevěnuje.[18] Pro úplnost nutno zmínit, že před existencí Nařízení bylo o těchto údajích referováno jako o tzv. citlivých údajích. Těmi se podle odborné literatury rozuměly takové údaje, které tvoří podmnožinu osobních údajů a u kterých musí být splněny dvě podmínky, aby se o ně mohlo jednat. Zaprvé se daná informace musí týkat identifikované či identifikovatelné osoby (a musí tedy jít o osobní údaj) a musí se jednat o jednu ze specifických informací taxativně vyjmenovaných zákonem (již jen proto je pro definici citlivého údaje/zvláštní kategorie citlivých údajů rozhodující spíše pojem jejich jednotlivých subtypů).[19]

Bližší pozornost ze všech uvedených zvláštních kategorií osobních údajů Nařízení bude práce s ohledem na další kapitoly věnovat pouze biometrickým údajům. Těmi se dle pracovní skupiny WP29 rozumí *„biologické vlastnosti, behaviorální rysy, fyziologické rysy, znaky živého organismu nebo opakovatelné úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné, bez ohledu na to, že technické metody jejich měření používané v praxi zahrnují určitou míru pravděpodobnosti"*[20], přičemž tuto definici lze z hlediska pracovní skupiny WP29 považovat za ustálenou, neboť na ni i nadále ve svých stanoviscích odkazovala.[21]

Biometrické údaje je možno dělit do několika kategorií, přičemž primárním hraničním určovatelem tohoto dělení je míra specifičnosti a určitelnosti rysů dotčených údajů. V tomto kontextu lze hovořit o tzv. silných biometrických rysech (například otisk prstu), slabých biometrických rysech (styl chůze – tyto biometrické rysy se projevují tím, že při vyvinutí určité snahy může dojít k jejich změně) a měkkých biometrických rysech (pouze pomocné identifikátory doprovázející zbylé dvě kategorie jako např. věk či pohlaví).[22] Další dělení biometrických údajů, které se v teorii objevuje, je dělení na statické biometrické údaje (tedy takové, které se v průběhu života člověka nemění – mezi ty řadíme například daktyloskopickou stopu), statické s testováním přítomnosti osoby (tzv. projev živosti) a dynamické (tedy takové biometrické údaje, které se mohou v průběhu života člověka změnit – mezi ty řadíme např. podpis člověka).[23]

---

[18] Srov. RÁMIŠ, V. in UŘIČÁŘ, M, RÁMIŠ V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 4.
[19] NONNEMANN, F. in KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL D.: *Zákon o ochraně osobních údajů. Komentář.* 1. vydání. Praha: C. H. Beck. 2021. Komentář k § 4.
[20] Srov. stanovisko pracovní skupiny WP 29, č. 4/2007 (WP 136).
[21] Srov. například stanovisko pracovní skupiny WP 29 z 27. dubna 2012, č. 3/2012 (WP 193).
[22] MORÁVEK, J. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR. 2019. 129 s.
[23] Op cit. sub 19 KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL D.: *Zákon o ochraně osobních údajů. Komentář.*

Biometrické údaje a jejich zpracování se po přijetí Nařízení těší stále větší pozornosti, neboť zatímco se jejich využívání i v pracovněprávních vztazích (např. docházkové systémy)[24] stává se snadněji přístupnou technologií stále častější, dle Nařízení je lze zpracovávat pouze ve speciálně stanovených případech taxativně vymezených v čl. 9 odst. 2 Nařízení, což klade zvýšené nároky na zaměstnavatele jakožto správce této zvláštní kategorie údajů. V této souvislosti lze ještě zmínit, že na mezinárodní úrovni jsou biometrické údaje vedle Nařízení řešeny ještě také v rámci úmluvy Rady Evropy o ochraně osob se zřetelem k automatizovanému zpracování osobních dat ze dne 28. ledna 1981, a to konkrétně ve znění jejího dodatkového protokolu č. 2.[25] Tento druhý protokol rozšířil čl. 6 dotčené úmluvy, a to tak, že do skupiny zvláštních údajů zařadil i biometrické údaje, které umožňují jedinečnou identifikaci fyzické osoby.

2.3. Subjekt osobních údajů

Dříve účinný právní předpis upravující oblast ochrany osobních údajů v České republice, tedy zákon č. 101/2000 Sb., o ochraně osobních údajů vymezoval subjekt údajů v ustanovení § 4 písm. d) jednoduše jako fyzickou osobu, k níž se osobní údaj vztahuje. ZOZOÚ tuto definici přejal a lze ji nalézt v ustanovení § 3 tohoto právního předpisu a Nařízení obsahuje definici subjektu údajů v rámci vymezení pojmu osobního údaje, tedy v čl. 4 odst. 1 Nařízení, podle kterého se jím rozumí každá identifikovaná či identifikovatelná osoba. Morávek uzavírá, že subjektem údajů je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat, zejména s odkazem na určitý identifikátor, kterým může být v podstatě cokoli od jména a příjmení, přes informaci o poloze až po jedinečné znaky člověka jako prvky fyziologické, genetické, ekonomické, kulturní či společenské identity.[26]

První důležitou otázkou při posuzování subjektu údajů je, zda se právní předpisy ochrany osobních údajů včetně Nařízení vztahují jen a pouze na fyzické osoby, nebo rovněž na osoby právnické. Již recitál č. (14) Nařízení uvádí, že: *„Toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby.“* Toto zdánlivě velmi striktní vyloučení aplikace Nařízení na právnické osoby má však dva limity. To proto, že Soudní

[24] Srov. stanovisko ÚOOÚ č. 1/2017. *Biometrická identifikace nebo autentizace zaměstnanců*. Věstník ÚOOÚ. 2018.
[25] První dodatkový protokol byl přijat v roce 2001 a v České republice je platný od 1. července 2004. Zmíněný druhý dodatkový protokol k úmluvě je z roku 2018 a Česká republika jej podepsala v říjnu téhož roku.
[26] MORÁVEK, J. op. cit. sub 22. 129 s.

dvůr[27] judikoval ještě před účinností Nařízení, že jednotlivým členským státům nic nebrání v tom, aby oblast působnosti vnitrostátních právních předpisů na ochranu osobních údajů vztáhly také na právnické osoby, nepůjde-li to do přímého rozporu s unijním právem.[28]

Druhým problematickým aspektem je aplikace Nařízení a souvisejících předpisů na podnikající fyzické osoby. V tomto kontextu je podstatný rozpor mezi přístupem ÚOOÚ a Ústavním soudem České republiky. Ten v jednom ze svých nálezů[29] uvedl, že: *„Uvedený zákon* (zákon č. 101/2000 Sb. – poznámka autora) *totiž vymezuje v § 1 (předmět úpravy) svoji osobní působnost tak, že se vztahuje na ochranu osobních údajů fyzických osob. Nechrání tedy osoby právnické. Pokud jde o fyzické osoby, které jsou podnikateli (…) lze usuzovat stejně, neboť z hlediska jejich statusu je nutno za rozlišovací kritérium považovat jejich činnost podnikatelskou.“* S tímto názorem se však v jednom ze svých stanovisek[30] neztotožnil ÚOOÚ, který v jeho samotném závěru stanovil, že: *„Údaje týkající se určitých nebo určitelných osob, živnostníků či příslušníků svobodných povolání, jsou osobními údaji ve smyslu zákona o ochraně osobních údajů. Jejich zpracování ve formě vedení veřejně dostupných registrů je sice upraveno řadou zvláštních zákonů, ovšem zákon o ochraně osobních údajů jako obecný předpis je nutno rovněž aplikovat, a to v těch částech daného zpracování, které zvláštními předpisy upraveny nejsou.“* Otázkou zůstává, zda nejde ÚOOÚ při posuzování povahy osobních údajů podnikajících fyzických osob příliš daleko. Funkčnost veřejně dostupných registrů a v nich zveřejňovaných informací vychází z dlouhodobě aprobovaných a uznávaných zásad materiální a formální publicity, a nedotýkají-li se proto jednotlivé informace o podnikající fyzické osobě osobnostní sféry její či jiné fyzické osoby, nelze na ně nahlížet jako na osobní údaje ve smyslu Nařízení.

Třetí a poslední historicky problematickou skupinou ochrany osobních údajů jsou zemřelí a nenarození (*nasciturus*). Pokud se zesnulých osob týče, před účinností Nařízení nebylo jejich postavení jako subjektu údajů jednoznačně řešeno a ÚOOÚ ve své praxi vydávání stanovisek dovodil, že se na ně částečně ochrana osobních údajů aplikovat bude.[31] V dnešní době však již tato debata není ani v aplikační praxi, ani akademicky zajímavá a rozporná, neboť recitál č. (27) Nařízení jednoznačně stanovil, že se Nařízení *„nevztahuje na osobní údaje*

[27] Soudním dvorem se rozumí jeden ze dvou soudů, kterými je tvořen Soudní dvůr Evropské unie, který je tvořen jedním soudcem za každý členský stát Evropské unie, a který má 11 generálních advokátů.
[28] Rozsudek Soudního dvora ze dne 6. listopadu 2003, sp. zn. C-101/2001, ve věci Lindqvist.
[29] Nález Ústavního soudu České republiky z 9. března 2004, sp. zn. Pl. ÚS 38/02.
[30] Stanovisko Úřadu pro ochranu osobních údajů č. 3/2011. 2011.
[31] Stanovisko ÚOOÚ č. 4/2012. 2012 a stanovisko ÚOOÚ č. 7/2002. 2002, 2005, 2009.

zesnulých osob. Členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zesnulých osob.“ Pokud se osob nenarozených (*nasciturus*) týče, v ochraně osobních údajů je obecně platná premisa, že se poskytuje od narození do smrti. To však neznamená, že žádné údaje ohledně *nascitura* chráněny nejsou, neboť před narozením dítěte, které již je samo subjektem údajů, mohou mnohé údaje o něm samotném představovat rovněž osobní údaje jeho rodičů, čím se *de facto* do působnosti, a tím také do ochrany Nařízení *nasciturus* dostává. To však vždy jen a pouze jakožto osobní údaj třetí osoby, v tomto případě rodičů.

2.4. Speciální subjekty dle Nařízení

Nařízení pracuje s mnoha různými pojmy a jeho definiční ustanovení, tedy článek 4 obsahuje 26 samostatných definic, mezi nimiž lze nalézt všemožné subjekty, kterých se více či méně právní úprava ochrany osobních údajů dotýká. Těmi nejdůležitějšími, kterým bude v této podkapitole věnována speciální pozornost, jsou správce osobních údajů[32], zpracovatel osobních údajů[33] a příjemce osobních údajů[34].

Správcem osobních údajů dle Nařízení rozumíme fyzickou nebo právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Dále platí, že jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Z uvedené definice je patrné, že správce se od zpracovatele osobních údajů liší především tím, že je to on, kdo určuje prostředky zpracování osobních údajů podle účelu stanoveného zákonem. Nařízení potom pouze rozlišuje, zda se subjekt stává správcem na základě vlastního volního rozhodnutí (například zavedení kamerového systému v budově), či zda se stává subjekt správcem v důsledku zákonných povinností (například zaměstnavatel, který má povinnosti vést určité evidence pro sociální či daňové účely; který musí vést evidenci pracovních úrazů etc.). Speciální případ správce osobních údajů jsou rovněž subjekty, které se jím stanou v důsledku své funkce či postavení v kombinaci se zákonným příkazem ke zpracování osobních údajů (například veřejné rejstříky).[35]

[32] Srov. čl. 4 odst. 7 Nařízení.
[33] Srov. čl. 4 odst. 8 Nařízení.
[34] Srov. čl. 4 odst. 9 Nařízení.
[35] MORÁVEK, J. op. cit. sub 22. 149 a 150 s.

Podle odborného stanoviska skupiny WP29 z roku 2010 č. 1/2010 platí, že aby mohl být subjekt považován za správce osobních údajů, musí kumulativně splnit tři základní definiční prvky, a sice, (i) že se musí jednat o fyzickou či právnickou osobu, orgán veřejné moci, agenturu nebo jakýkoli jiný subjekt, který (ii) sám nebo společně s jinými (iii) určuje účel a prostředky zpracování.[36]

K prvnímu z uvedených prvků se stanovisko vyjadřuje zejména v rovině odpovědnostní. Pracovní skupina WP 29 zdůraznila, že je především nutné poskytnout subjektům údajů, tedy osobám, o jejichž práva při zpracování osobních údajů jde, stálý a spolehlivý referenční subjekt, na který se budou moci obrátit s uplatňováním všech svých práv při ochraně jejich osobních údajů. Stejně tak v případě, že k porušení těchto práv dojde, resp. že dojde ke zneužití těchto osobních údajů subjektu, slouží správce jako ten, po kterém lze v souvislosti s uvedeným požadovat například náhradu újmy způsobené v důsledku jeho škodného jednání.

Ve vztahu k druhému prvku definice správce osobních údajů se předmětné stanovisko spíše věnuje problémům, které mohou při posuzování, zda někdo určuje účel zpracování sám či společně s jinými, vzniknout. Vyplývá z něj přitom, že podstatná je materialita zkoumaného vztahu, tedy i když se například smluvně strany zaváží, že jedna smluvní strana vystupuje pouze jako zpracovatel pro smluvní stranu druhou, pořád se musí posuzovat, jakou činnost tato smluvní strana skutečně vykonává a zda tak reálně neexistují dva subjekty, které určují účel zpracování, a to společně.

Třetí prvek stanovisko rozebírá ze všech uvedených nejpodrobněji a věnuje se tomu, co znamená „*určit*“, jakož i co znamená v dané definici „*účel*“. K určení účelů a prostředků stanovisko v podstatě podrobněji rozebírá shora označené tři případy, ve kterých se určitý subjekt dostane do pozice správce, a získá tak svou legitimitu, tedy jak funguje určení v případě výslovné zákonné pravomoci a povinností, jak v případě implicitní pravomoci a jak v případě skutečného vlivu, kdy se někdo do role správce dostane například v důsledku smluvního ujednání.

Důležité přitom vždy je, že určení účelu a prostředku zpracování je povinností správce, se kterou je spojena i potenciální zákonná odpovědnost. Pokud totiž dojde k nesprávnému či záměrně špatnému „určení“, může v důsledku toho dojít k poškození práv a oprávněných zájmů

[36] Stanovisko pracovní skupiny WP29 z 16. února 2010 č. 1/2010 (WP 169).

subjektů údajů, čímž dochází k aktivací dříve latentní odpovědnosti správce. K účelu se pak podrobně vyjadřuje i odborná literatura, ve které se uvádí, že existují tři základní skupiny účelů zpracování osobních údajů.[37] První z těchto skupin jsou případy, kdy je účelem zpracování osobních údajů zákonná povinnost či rozhodnutí orgánu veřejné moci. V takovém případě je typické, že správce nemá možnost se svobodně rozhodnout, zda bude či nebude osobní údaje zpracovávat, neboť tak učinit musí. Druhou skupinou jsou případy, kdy si účel zpracování správce určuje dle své vlastní vůle. Jedná se tedy o fakultativní možnost správce, přičemž nejsou nastaveny ani zákonné podmínky takového zpracování (například na jak dlouhou dobu může správce dané údaje zpracovávat). Třetí skupina v sobě pak pojí obě předchozí. Je pro ni totiž typické, že rozhodnutí správce o tom, zda bude zpracovávat osobní údaje, je sice fakultativní, ale jakmile jej jednou učiní a začne se zpracováním, musí tak již činit na základě jasně vymezených kritérií, která nelze jeho svobodnou vůlí modifikovat.

K tomu je potřebné rovněž zdůraznit, že účel zpracování osobních údajů velmi úzce souvisí s otázkou zákonnosti takového zpracování. To plyne již jen z textace čl. 6 odst. 1 Nařízení, ve kterém jsou taxativně vyjmenovány právní důvody zpracování osobních údajů, tedy účely, za kterými správce osobní údaje subjektů údajů zpracovává.[38]

Správce osobních údajů je vedle odborné literatury a výkladové činnosti pracovní skupiny WP 29 historicky rovněž vymezen také judikaturou, která tento pojem vnímá poměrně extenzivním způsobem. Důvodem k tomu je řádné naplnění definiční pasáže správce osobních údajů, která říká, že jím může být i *jiný subjekt*.[39] Aby se tedy někdo stal správcem osobních údajů, musí především určit účel a prostředky zpracování osobních údajů, jinými slovy musí kvalifikovaně rozhodnout o jejich zpracování.[40] V této souvislosti je pouze pro úplnost třeba zmínit, že správcem se subjekt nestává jen proto, že má ke zpracovaným osobním údajům přístup.[41]

Pokud se prostředků zpracování týče, rozumí se tím jednoduše cokoli, čím je možné zpracování osobních údajů uskutečnit (od počítačového programu, přes vyplňování dotazníků až po ústní pohovor, ze kterého je zaznamenán písemný protokol). V souvislosti se vším shora

[37] MORÁVEK, J. op. cit. sub 22. 150 s.
[38] Pro zvláštní kategorii osobních údajů, a tedy i pro biometrické údaje se však v této rovině uplatní čl. 9 Nařízení.
[39] Rozhodnutí SDEU ze dne 13. května 2014, sp. zn. C-131/12 ve věci *Google Inc.vs. AEPD*.
[40] Op cit. sub 19 KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář.* Komentář k čl. 4.
[41] Rozhodnutí SDEU ze dne 10. července 2018, sp. zn. C-25/17 ve věci *Jehovan Todistajat* a rozhodnutí SDEU ze dne 5. června 2018, sp. zn. C-210/16 ve věci *Facebook Fan Page*.

uvedeným je potřeba ještě upozornit na čl. 24 až 26 Nařízení, které upravují blíže některé další povinnosti správce, které musí dodržovat. Mezi ty patří povinnosti vznikající při činnosti tzv. společných správců,[42] povinnosti zástupců správců, kteří nejsou usazeni v Evropské unii a povinnosti správce související s využíváním služeb zpracovatele.

Zpracovatel je v Nařízení definován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Shora zmíněné stanovisko pracovní skupiny WP 29 pak uvádí, že *„Existence zpracovatele závisí na rozhodnutí přijatém správcem, který může rozhodnout, že údaje budou zpracovány v rámci jeho organizace, například zaměstnanci oprávněnými ke zpracování údajů přímo podléhajícími správci (viz naopak čl. 2 písm. f), nebo přenese veškeré činnosti spojené se zpracováním či jejich část na externí organizaci, tj. jak uvádí důvodová zpráva pozměněného návrhu Komise, „samostatnou právnickou osobou jednající jeho jménem.“*[43]

Z toho lze vyvodit jeden ze dvou základních definičních znaků, který musí být naplněn k tomu, aby daný subjekt vystupoval v pozici zpracovatele ve smyslu Nařízení, a sice, že se musí jednat o osobu odlišnou od správce, což také znamená, že zpracovatelem nikdy nebude osoba, která je ke správci v pracovněprávním či obdobném vztahu (statutární orgán). Tato skutečnost je přitom z hlediska Nařízení a právní úpravy ochrany osobních údajů obecně velmi významná, neboť ze vztahu správce-zpracovatel vyplývají mnohé povinnosti, které musí být řádně splněny k tomu, aby se ani jeden z těchto subjektů nemohl dopustit žádného protiprávního jednání, jak například plyne z čl. 28 Nařízení. K povinnostem vznikajícím při zpracování osobních údajů se však tato práce blíže věnuje až v následující kapitole.

Druhým definičním znakem zpracovatele pak je, že tato osoba zpracovává osobní údaje „pro správce“. I z toho tak vyplývá, že základním stavebním kamenem definice zpracovatele a jeho činnosti v oblasti ochrany osobních údajů je zákon na straně jedné a jeho smluvní vztah se správcem, na jehož základě pro něj vykonává určitou činnost v rámci procesu zpracování osobních údajů, na straně druhé. Aby přitom byl daný subjekt v pozici zpracovatele, stačí, aby pro správce vykonával alespoň jednu činnost v rámci zpracování osobních údajů od jejich shromáždění, kterým zpracování začíná, až po jejich likvidaci, kterou zpracování osobních údajů končí.

[42] Společní správci jsou upraveni v čl. 26 Nařízení a rozumí se jimi jednoduše dva či více správců, kteří společně stanoví účely a prostředky zpracování. Společní správci mezi sebou dle dotčeného ustanovení vždy musí vymezit své podíly na případné odpovědnosti vzniklé vůči subjektům údajů.
[43] Stanovisko pracovní skupiny WP29 z 16. února 2010 č. 1/2010 (WP 169). 23 s.

Rozhodné však zůstává primárně to, že zpracovatel osobních údajů jedná na základě pověření pro jiný subjekt, tedy správce, jenž je mj. i odpovědný za to, že zpracovatel je důvěryhodným subjektem, který svou činnost bude vykonávat řádně, a který poskytuje dostatečné záruky k tomu, aby nedošlo ke zneužití zpracovávaných osobních údajů.[44]

Vzhledem ke skutečnosti, že zpracovatel se může podílet jen na jedné konkrétní činnosti v rámci celého procesu zpracování osobních údajů, přišlo Nařízení s výslovnou legislativní úpravou tzv. řetězení zpracovatelů.[45] Možnost aplikovat řetězení zpracovatelů počítá s udělením souhlasu ze strany správce osobních údajů. Tento údaj může být podle čl. 28 odst. 2 Nařízení buďto konkrétní (tedy správce povolí předem určený subjekt, na který se bude zpracování řetězit), nebo může být udělen obecně (v takovém případě je však zpracovatel povinen správce vždy informovat o všech zamýšlených změnách, neboť ten může proti řetězení podat námitky). V případě, že správce tento souhlas nedá a zpracovatel i přesto přistoupí k užití třetí osoby provádějící jednu z činností při zpracování osobních údajů, odpovídá za ni zpracovatel, jako kdyby ji vykonával sám. Naopak pokud je řetězení *a priori* povoleno a správce s ním vyslovil souhlas, je povinen zajistit, aby i řetězený zpracovatel splňoval všechny záruky a podmínky, které musí splňovat i zpracovatel původní.

Poslední ze zmíněných zvláštních subjektů v oblasti ochrany osobních údajů je tzv. příjemce osobních údajů. Příjemcem je dle Nařízení: *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování“*[46] Podstatné ve vztahu k příjemci především je, že se vždy musí jednat o osobu odlišnou od správce a zpracovatele osobních údajů, jakož i od osob

[44] Srov. čl. 28 Nařízení.
[45] Vizte čl. 28 odst. 2, odst. 3 písm. d) a odst. 4 Nařízení: *„Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky. (...) Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel: d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4; (...) Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.”*
[46] Srov. čl. 4 odst. 9 Nařízení.

vykonávajících u správce či zpracovatele jednotlivé činnosti zpracování (zaměstnanci, členové statutárního orgánu). Příjemcem rovněž nikdy nebudou orgány veřejné moci, které předmětné údaje získávají v rámci jim svěřené pravomoci (typicky například Česká správa sociálního zabezpečení při získávání informací od zaměstnavatelů o jejich zaměstnancích).

2.5. Zpracování osobních údajů

Posledním pojmem, jenž bude v této práci podrobně definován a který je oblasti ochrany osobních údajů velmi podstatný, je zpracování osobních údajů. Dle Nařízení se zpracováním rozumí *jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*.[47] To v podstatě také odpovídá oficiální odpovědi na téma „Co se rozumí zpracováním osobních údajů“ zveřejněné na stránkách Evropské komise.[48] Důležitost tohoto pojmu vyplývá i z vymezení předmětu a cílů a věcné působnosti Nařízení, neboť podle nich Nařízení stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů.[49] Věcně se Nařízení přitom vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.[50] S ohledem na vymezení věcné působnosti Nařízení je v souvislosti se zpracováním velmi důležitý rovněž pojem evidence, kterou je *jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska*.[51]

Zpracování osobních údajů tak lze provádět jak automatizovanými procesy, typicky prostřednictvím výpočetní techniky, jež usnadňuje celou proceduru zpracování prostřednictvím elektrifikace (nejvíce rozšířeným příkladem takto automatizovaného zpracování budou zaměstnavatelské systémy elektronické evidence pracovní doby, dovolené na zotavenou, doby

[47] Srov. čl. 4 odst. 2 Nařízení.
[48] Zde je uvedeno, že: *„Termín „zpracování“ pokrývá širokou škálu operací prováděných na osobních údajích, ať už manuálně, nebo automatizovaně. Zahrnuje shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení osobních údajů.“* Dostupné online na: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_cs
[49] Srov. čl. 1 odst. 1 Nařízení.
[50] Srov. čl. 2 odst. 1 Nařízení.
[51] Srov. čl. 4 odst. 6 Nařízení.

strávené na dočasné pracovní neschopnosti), tak i neautomatizovanými, tedy způsobem manuálním (například vedení osobního spisu zaměstnance, který je v tištěné podobě zařazen v kartotéce nebo spisovně). Uvedená skutečnost vyplývá mj. i z recitálu (15) Nařízení, kde je uvedeno, že: *„S cílem zabránit vzniku vážného rizika obcházení by ochrana fyzických osob měla být technologicky neutrální a nezávislá na použitých technologiích. Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Záznamy nebo soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určených hledisek, by do oblasti působnosti tohoto nařízení spadat neměly.“*

Aby se jednalo o zpracování osobních údajů ve smyslu Nařízení a ZOZOÚ, musí tato činnost vykazovat určité prvky soustavnosti a musí být vedena předem jasně stanoveným a vymezeným účelem. Jinými slovy, pokud se jedná pouze o nahodilé shromažďování údajů, které není činěno s konkrétním cílem například dosáhnout vytvoření specifické evidence či získané osobní údaje dále používat, nebude se jednat o zpracování.[52] Účel zpracování osobních údajů je také pojítkem mezi jednotlivými činnostmi, které pod zpracování osobních údajů lze podřadit, jako například shromažďování, analýza, jejich třídění, uložení a následná likvidace.[53] Stejně tak je uvedeno rovněž ve stanovisku ÚOOÚ č. 4/2013 z října 2013, kde se mj. píše, že: *„Je-li charakteristikou konkrétního nakládání systematičnost, jedná se o zpracování osobních údajů. K pravidelným znakům systematičnosti, nikoliv však definičním, patří opakovanost či jednotící účel.“*[54] Systematičnost, opakovanost a účel jsou tak pomocnými atributy, které slouží k rozlišování mnohdy velmi jemné hranice mezi nahodilou činnosti související s osobními údaji, která však nebude spadat do působnosti Nařízení a mezi zpracováním osobních údajů *stricto sensu*.[55]

Jak dále plyne již ze samotné definice obsažené v Nařízení, zpracování osobních údajů se skládá ze široké škály operací, které může správce, resp. zpracovatel, s osobními údaji činit. Pouze pro úplnost lze uvést, že dnes již neúčinný ZOOÚ mj. definoval, co znamenají jednotlivé pojmy představující subkategorie zpracování.

[52] Srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J.: *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář.* Praha: Wolters Kluwer. 2017. 86 s.
[53] MORÁVEK, J. op. cit. sub 22. 132 s.
[54] Stanovisko Úřadu pro ochranu osobních údajů z října 2013, č. 4/2013.
[55] K systematičnosti blíže například rozhodnutí NSS ze dne 20. srpna 2014, č. j. 6 As 144/2013-34.

Těmi nejvýznamnějšími z nich jsou samozřejmě shromažďování, uchovávání (zaznamenání, uspořádání, strukturování či uložení), použití (nahlédnutí, zpřístupnění, šíření, seřazení, zkombinování) a likvidace (výmaz, zničení). ZOOÚ přitom definoval shromažďování, a to jako systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování;[56] uchovávání, a to jako udržování údajů v takové podobě, která je umožňuje dále zpracovávat[57] a likvidaci, a to jako fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.[58] I s ohledem na takto široké vymezení operací, které pod zpracování spadají, ÚOOÚ ve své rozhodovací praxi dospěl k tomu, že je pojem zpracování potřebné vykládat co možná nejvíce extenzivně.[59]

Závěrem této podkapitoly je ještě potřeba zmínit také pojem tzv. automatizovaného rozhodování a profilování. Profilování představuje zvláštní způsob zpracování osobních údajů, kterému lze dle čl. 4 odst. 4) Nařízení rozumět jako jakékoli formě automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.[60]

Jak přitom plyne z čl. 22 Nařízení, tento právní instrument rozlišuje tři základní pozice profilování, a to (i) profilování obecné, (ii) profilování směřující k rozhodování a (iii) profilování, které je součástí výhradně automatizovaného rozhodování. Profilování má v Nařízení svou speciální úpravu, neboť z hlediska rizik a dotknutelnosti subjektů údajů může profilování představovat mnohem větší zásah do jejich práv a oprávněných zájmů než jen pouhé a běžné zpracovávání osobních údajů. To vše zejména se stále větším rozmachem techniky a tzv. *Big Data*,[61] pomocí kterých lze také významně ovlivnit konkurenční prostředí v určitém

[56] Srov. ustanovení § 4 písm. f) ZOOÚ.
[57] Srov. ustanovení § 4 písm. g) ZOOÚ.
[58] Srov. ustanovení § 4 písm. i) ZOOÚ.
[59] Op cit. sub 19 KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář.* Komentář k čl. 4.
[60] Tato definice použitá v Nařízení vychází mj. z doporučení Rady Evropy č. CM/Rec (2010)13.
[61] *Big Data* (v češtině také velká data) představují obrovské množství dat, která mohou být analyzována za účelem vysledování určitých vzorců, postupů a trendů propojených s chováním lidí, jež právě až při zpracování ve velkém rozsahu mohou představovat hodnotný zdroj informací. Tak například informace o tom, že se v jedné domácnosti nejčastěji spustí televize v časovém rozmezí od 13:00 do 13:30 nemá žádnou marketingovou hodnotu. Pokud ale při analýze *Big Data* dospějeme k závěru, že například 98 % všech domácností v Praze zapíná v tomto časovém rozmezí televizi, jedná se z hlediska marketingu o významnou informaci, neboť provozovatelé televizních služeb vědí, že přesně v tomto časovém rozmezí má největší smysl přehrát obsah s co nejvyšším poměrem marketingových sdělení a reklam.

odvětví, kdy podnikatel, který profilování užívá a má k dispozici možnost úspěšné a spolehlivé diferenciace mezi potenciálními zákazníky, mnohem lépe dokáže cílit svou reklamu a ovlivnit rozhodování spotřebitele pomocí cíleného marketingu.

Automatizované rozhodování velmi úzce souvisí jak s pojmem profilování (které *de facto* je jeho výsledkem) a automatizovaného zpracování osobních údajů a nastává v situaci, kdy jsou určitá rozhodnutí založena výhradně na automatizovaném zpracování, přičemž dané rozhodnutí musí mít vůči subjektu údajů významné právní účinky. Automatizované rozhodování je z hlediska ochrany osobních údajů proces, který není za všech okolností a bez dalšího povolen a k jehož užití nutno přistupovat velmi restriktivně.[62]

Právní odvětví ochrany osobních údajů samozřejmě obsahuje mnohem více pojmů, z nichž některé jsou velmi problematické a jejich správné uchopení je tak poměrně složité, pročež by si i tyto zasloužily, aby jim byla věnována větší pozornost. Pro účely této práce, která bude ve své stěžejní části mířit zejména na ochranu osobních údajů v pracovněprávních vztazích, je však podrobné vymezení shora popsaných pojmů postačující a po jejich bližším pochopení se nyní práce může věnovat již více praktickým otázkám. Než však bude nasnadě začít se podrobně zabývat problematikou ochrany osobních údajů v pracovněprávních vztazích se zaměřením na opakovaně zmiňovanou biometriku, bude v následující fázi této práce kladen důraz na detailnější popis jednotlivých povinností při zpracování osobních údajů vznikajících na straně správce a zpracovatele osobních údajů a všech nejdůležitějších práv, která jsou Nařízením či vnitrostátní legislativou přiznávána subjektům údajů.

[62] K výkladu pojmu automatizovaného zpracování a jeho restriktivnímu pojetí srov. například rozhodnutí SDEU ze dne 6. listopadu 2003, sp. zn. C-101/01, ve věci *Lindqvist* nebo také rozhodnutí NSS ze dne 30. ledna 2013, č. j. 7 As 150/2012-35.

3. Povinnosti při zpracování osobních údajů

Jedním z hlavních dopadů Nařízení je, že oproti Směrnici velmi důkladně rozepsalo povinnosti správců a zpracovatelů osobních údajů. Zatímco tedy práva subjektu údajů, která jsou popsána v další kapitole, byla tedy pouze specifikována nebo lépe vysvětlena, ale zůstala v obdobném rozsahu, povinnostem správce a zpracovatele osobních údajů věnoval evropský zákonodárce mnohem větší pozornost.

Dnes jsou základní povinnosti správců a zpracovatelů osobních údajů normovány v článku 5 Nařízení, který se věnuje zásadám, na nichž je celá oblast ochrany osobních údajů postavena.[63]

V Čl. 5 Nařízení tak lze identifikovat šest základních povinností/zásad souvisejících se zpracováním osobních údajů, kterými jsou:

(i) Dodržování principu zákonnosti, korektnosti a transparentnosti – s tím souvisí možná nejdůležitější povinnost v oblasti ochrany osobních údajů, kterou je stanovení účelu zpracování a zpracování pouze v souladu s tímto účelem;[64][65]

(ii) Zpracování osobních údajů takovým způsobem, aby byl slučitelný s účelem zpracování a jejich shromáždění pouze pro určité, výslovně vyjádřené a legitimní účely;[66][67]

(iii) Zpracování přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu ke stanovenému účelu – tzv. minimalizace údajů;[68][69]

(iv) Přesné a aktualizované zpracování – tj. je kladen důraz na to, aby zpracované osobní údaje byly správné a nikoli zavádějící vzhledem ke stanovenému účelu

[63] MORÁVEK, J. op. cit. sub 22. 189 s. a dále čl. 5 odst. 2 Nařízení. K tomu také Op cit. sub 18 UŘIČÁŘ, M, RÁMIŠ V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 5, kde se uvádí, že: *„Ustanovení čl. 5 obsahuje v odstavci 1 základní zásady zpracování osobních údajů. Odstavec druhý pak přenáší odpovědnost za dodržení základních zásad na správce a ukládá mu povinnost být schopen doložit dodržování těchto zásad.“*

[64] Srov. čl. 5 odst. 1 písm. a) Nařízení.

[65] K tomu také blíže pokyny pracovní skupiny WP29 ze dne 29. listopadu 2017, ve znění ze dne 11. dubna 2018 č. (WP 260) k transparentnosti podle Nařízení.

[66] Srov. čl. 5 odst. 1 písm. b) Nařízení.

[67] K tomu také blíže stanovisko pracovní skupiny WP29 ze dne 2. dubna 2013 č. 3/2013 k účelovému omezení.

[68] Srov. čl. 5 odst. 1 písm. c) Nařízení.

[69] K tomu také blíže stanovisko ÚOOÚ č. 6/2009: Ochrana soukromí při zpracování osobních údajů. Listopad 2009, aktualizace únor 2014.

(tj. nemusí se jednat o informace pravdivé, jen nesmí být nepřesné pro účel zpracování);[70]

(v) Zpracování pouze po dobu, po kterou je to nezbytné vzhledem k účelu zpracování;[71][72] a

(vi) Zpracování osobních údajů takovým způsobem, aby bylo zajištěno jejich zabezpečení a ochrana pomocí technických a organizačních opatření – tzv. princip integrity a důvěrnosti.[73][74]

V následující části se bude tato práce podrobně zabývat všemi jednotlivými povinnostmi tak, jak je lze extrahovat z čl. 5 Nařízení. Předně však bude věnována pozornost především titulům, na jejichž základě je vůbec možné osobní údaje zpracovávat.

3.1. Právní tituly pro zpracování osobních údajů

Jak plyne již z Listiny základních práv a svobod České republiky, osobnost člověka, jeho soukromí a nedotknutelnost jeho osoby (což jsou všechno maximy velmi úzce spojené s ochranou osobních údajů) jsou zaručeny, každý má právo na jejich zachování a omezeny mohou být jen v případech stanovených zákonným předpisem.[75] Jakým způsobem lze základní lidská práva a svobody omezovat, resp. jak lze těmto určovat mantinely a nakládat s nimi v rámci jejich ochrany, pak podrobně normuje čl. 4 a okrajově rovněž čl. 2 Listiny základních práv a svobod. Již na základě této ústavněprávní roviny ochrany osobnosti a soukromí je zřejmé, že aby správce mohl zpracovávat osobní údaje a nakládat s nimi, musí k tomu vždy mít dostatečný právní titul předpokládaný zákonem, na jehož základě tak činí.

V této rovině je rozhodující především čl. 6 odst. 1 Nařízení (obecná úprava právních titulů pro zpracování osobních údajů) a čl. 9 odst. 2 Nařízení (úprava právních titulů pro zpracování zvláštní kategorie osobních údajů). Čl. 6 odst. 1 Nařízení (stejně jako to dříve činil

[70] Srov. čl. 5 odst. 1 písm. d) Nařízení.
[71] Srov. čl. 5 odst. 1 písm. e) Nařízení.
[72] S omezením uložení velmi úzce souvisí otázka anonymizace osobních údajů. K tomu srov. stanovisko pracovní skupiny WP29 ze dne 10. dubna 2014 č. 5/2014 (WP216) k technikám anonymizace.
[73] Srov. čl. 5 odst. 1 písm. f) Nařízení.
[74] Tato povinnost, resp. zásada, velmi úzce souvisí i s dalšími povinnostmi dle Nařízení, jako např. povinnost dle čl. 30 Nařízení k vedení záznamů o činnosti, povinnost ohlašovací a oznamovací ve smyslu čl. 33 a 34 Nařízení apod.
[75] Srov. čl. 7 Listiny základních práv a svobod vztahující se k nedotknutelnosti osoby a jejího soukromí a čl. 10 Listiny základních práv a svobod normující práva související s ochranou lidské důstojnosti, osobní cti, dobré pověsti a vlastního jména.

§ 5 odst. 2 ZOOÚ) vyjmenovává právní tituly pro zpracování taxativně, přičemž se jedná konkrétně o:

(i) Souhlas subjektu údajů se zpracováním;[76]

(ii) Nezbytnost zpracování z důvodu plnění smlouvy, jejíž smluvní stranou je subjekt údajů;[77]

(iii) Nezbytnost zpracování pro splnění právní povinnosti, která se na správce vztahuje;[78]

(iv) Nezbytnost zpracování pro ochranu životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby;

(v) Nezbytnost zpracování pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci; a

(vi) Nezbytnost zpracování pro účely oprávněných zájmů příslušného správce či třetí osoby.[79]

Čl. 9 Nařízení *a priori* stanoví, že se zakazuje zpracování osobních údajů vypovídajících o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. I tento zákaz je však možné prolomit, je-li naplněn jeden ze zákonných titulů dle čl. 2 odst. 9 Nařízení.[80] Již na tomto místě lze ale říct, že právní tituly pro zpracování zvláštní kategorie osobních údajů jsou *de facto* totožné s těmi pro zpracování běžných osobních údajů.

[76] K tomu srov. např. stanovisko pracovní skupiny WP 29 z 13. července 2011 č. 15/2011 (WP187) k definici souhlasu, nebo alternativně stanovisko Evropského sboru pro ochranu osobních údajů z 4. května 2020 k souhlasu dle Nařízení č. 5/2020.
[77] K tomu srov. např. stanovisko pracovní skupiny WP 29 z 9. dubna 2014 č. 6/2014 (WP217) k pojmu oprávněných zájmů podle Směrnice. 16 a 17 s.
[78] Ibid. 19 s.
[79] Ibid.
[80] K těmto srov. kapitola 3.2 této rigorózní práce.

3.1.1. Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů jako samostatný titul pro jejich zpracování je velmi problematickým právním titulem. Dle čl. 4 odst. 11) Nařízení se souhlasem rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Pro souhlas subjektu údajů se zpracováním osobních údajů Nařízení jako pro jediný titul zpracování normuje další specifické podmínky možnosti jeho užití. Ty jsou blíže popsány v čl. 7 Nařízení, ze kterého plyne, že:

(i) Správce osobních údajů musí být schopen doložit, že subjekt údajů souhlas se zpracováním svých osobních údajů skutečně udělil;[81]

(ii) Za předpokladu, že je prohlášení k souhlasu se zpracováním osobních údajů předloženo subjektu údajů takovou formou, že se týká i jiných skutečností, než jen zpracování osobních údajů v důsledku udělení souhlasu, musí být ta část, která se týká zmíněného prohlášení naprosto zřetelně a jasně oddělená od těchto ostatních skutečností;[82]

(iii) Subjekt údajů musí mít možnost udělený souhlas kdykoli odvolat, přičemž o této možnosti musí být subjekt údajů dopředu informován – v této souvislosti je rovněž podstatné, že odvolat udělený souhlas musí být stejně jednoduché, jako bylo tento souhlas poskytnout;[83]

(iv) Při posuzování, zda byl souhlas poskytnut svobodně, musí být brána na zřetel skutečnost, zda plnění smlouvy či poskytnutí služby je podmíněno souhlasem se zpracováním, které není pro plnění smlouvy či poskytnutí služby nezbytné.[84]

Pouze pro úplnost lze uvést, že pokud obdobná normativní pravidla v úpravě předcházející Nařízení absentovala, nedá se říct, že by neexistovala a nebyla vymáhána. Uvedená skutečnost plyne například z postoje ÚOOÚ k zahrnutí souhlasu do smlouvy nebo

[81] K tomu srov. také recitál (42) Nařízení, kde se uvádí, že: *„Pokud je zpracování založeno na souhlasu subjektu údajů, měl by být správce schopen prokázat, že subjekt údajů vyjádřil s danou operací zpracování souhlas."*
[82] K tomu srov. stanovisko Evropského sboru pro ochranu osobních údajů č. 5/2020, kde je uvedeno, že: *„Je-li souhlas požadován v rámci (tištěné) smlouvy, žádost o souhlas by měla být jasně odlišitelná od jiných záležitostí."*
[83] K odvolání souhlasu srov. stanovisko pracovní skupiny WP 29 o souhlasu č. 15/2011 (WP 187). Alternativně také stanovisko pracovní skupiny WP 29 č. 5/2005 (WP 115), o používání lokalizačních údajů. 7 s.
[84] K tomu srov. také stanovisko pracovní skupiny WP 29 č. 2/2017 (WP 249) o zpracování údajů na pracovišti.

všeobecných obchodních podmínek, což byl postup, který nebyl ze strany ÚOOÚ vnímán pozitivně.[85]

V následujícím čl. 8 Nařízení pamatuje na specifikum dnešní pokrokové a moderní doby, kdy stanoví speciální podmínky pro udělování souhlasu ze strany dětí v souvislosti se službami informačních společností – obecné pravidlo říká, že je-li dítě mladší než 16 let, vždycky je takový souhlas zákonný pouze v případě, kdy jej za něj poskytne zákonný zástupce dotčeného dítěte. Členské státy přitom mají možnost snížit tuto hranici až na 13 let. Tato legislativní úprava je zohledněna rovněž v recitálu (38) Nařízení, kde se píše, že děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů, a to především pokud se jedná o cílený marketing.

Všechny shora uvedené podmínky jsou stejně jako speciální ochrana dětí rovněž zmíněny přímo v recitálech Nařízení, a to konkrétně v recitálech (32), (33), (42) a (43). I z těchto recitálů plyne, za jakých podmínek je souhlas platný a jaké podmínky musí být při udělování souhlasu zajištěny, aby mohl být považován za zákonný. Je zde rovněž zdůrazněno (což v čl. 7 i čl. 8 Nařízení chybí), že vyjádření souhlasu by nemělo představovat platný právní důvod se zpracováním osobních údajů ve zvláštních případech existence jakékoli subordinace mezi subjektem údajů a správcem (například když je správcem orgán veřejné moci).[86] Neméně důležité je, že recitály explicitně stanoví, že souhlas nelze považovat za zákonný, když subjekt údajů nemusí učinit žádnou aktivní činnost k tomu, aby souhlas udělil. V dnešní době tak již není možné (i když byla podobná praxe dříve naprosto běžná), že souhlas subjektu údajů je před vstupem například na určitou webovou stránku již zaškrtnutý a subjekt údajů musí vyvinout jakoukoli vlastní aktivitu k tomu, aby udělení souhlasu odmítl, přičemž stejná pravidla se vztahují i na tzv. cookies, kterým se však tato práce ve větší podrobnosti věnovat nebude.

Souhlas se zpracováním osobních údajů jako právní titul pro jejich zpracování má také zásadní vztah ke všem ostatním právním titulům zpracování vyjmenovaným v čl. 6 Nařízení. Pokud se správce rozhodne založit zpracování za určitým účelem na základě souhlasu subjektu údajů, musí vždy počítat s tím, že tento souhlas může být ze strany subjektu údajů stejně jednoduše odvolán (vizte shora čl. 7 Nařízení). Pokud k tomu v jakémkoli případě dojde,

[85] Stanovisko ÚOOÚ č. 2/2011: *Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy*. Srpen 2011, aktualizace únor 2014.
[86] Srov. recitál (42) a recitál (43) Nařízení.

správce údajů nemůže v jejich zpracování pokračovat, pokud k takovému postupu nemá jiný právní titul. Již jen proto je velmi důležité, aby správce vždy na samém začátku zpracování důsledně promyslel, jaký právní titul je v daném případě nejvhodnější použít a v případě potíží s jeho identifikací nesklouzával k užití souhlasu jako jakéhosi univerzálního právního titulu.[87] V této souvislosti je ještě rovněž důležité doplnit, že souhlas nemá v systematice jednotlivých titulů pro zpracování osobních údajů žádné specifické postavení.[88]

Poslední věc, kterou je ve vztahu k souhlasu se zpracováním osobních údajů jako samostatnému titulu pro jejich zpracování potřeba zmínit, je, že se z hlediska právní vědy jedná o právní jednání v soukromoprávním smyslu slova. To mj. znamená, že kromě shora uvedených podmínek dle Nařízení musí každý souhlas rovněž splňovat podmínky právního jednání dle OZ, neboť pokud by jakákoli z nich nebyla splněna, mohl by být souhlas považován za relativně či absolutně neplatné právní jednání. Z tohoto důvodu musí být každý souhlas se zpracováním učiněn svobodně, musí představovat jasný projev vůle, musí být určitý a srozumitelný a nesmí být učiněn v tísni, v omylu ani z donucení.[89] Souhlas musí být zároveň udělen osobou k tomu způsobilou a nesmí být získán v rozporu s dobrými mravy. Zejména hledisku svobody v rozhodování byla věnována velká pozornost také Evropským sborem pro ochranu osobních údajů, který určil, že o nesvobodný souhlas se může jednat především v situaci, kdy je udělen v rámci nerovnovážného stavu, když je jeho udělení podmínkou pro určité plnění, v případě tzv. granularity a v případě, kdy v souvislosti se souhlasem (zejména jeho odvolání) hrozí jakákoli újma.[90]

Nerovnovážným stavem typicky je, když správce vystupuje v pozici orgánu veřejné moci, jak již zmíněno shora. Evropský sbor pro ochranu osobních údajů však ve svém pokynu č. 05/2020 k souhlasu podle Nařízení uvádí, že podobná situace může nastávat rovněž v souvislosti se zaměstnáním, neboť zaměstnanci jsou ve vztahu podřízenosti vůči nadřízenému zaměstnavateli. Na tuto okolnost pamatuje rovněž samotné Nařízení v čl. 88, který dává členským státům možnost, aby v nich vnitrostátními předpisy či kolektivními smlouvami byly stanoveny konkrétnější pravidla pro ochranu osobních údajů zaměstnanců jako slabší strany. Takto mohou členské státy činit v souvislosti se zaměstnáním, zejména za účelem náboru,

[87] Srov. pokyny Evropského sboru pro ochranu osobních údajů z 4. května 2020 č. 05/2020 k souhlasu podle Nařízení. 26 s.
[88] Srov. např. stanovisko ÚOOÚ č. 3/2014: *K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti*. 2014.
[89] K tomu srov. také recitál (32) Nařízení.
[90] Op. cit. Sub. 88 až 13 s.

plnění pracovní smlouvy, včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru. To jinými slovy znamená, že tato speciální pravidla mohou členské státy nastavit pro celý proces existence pracovněprávního vztahu.

Podmíněností, která rovněž může evokovat absenci svobody při udělení souhlasu se zpracováním osobních údajů, se rozumí opakovaně zmiňovaná situace, kdy např. podnikatel podmíní plnění smlouvy či poskytnutí služby udělením souhlasu, i když ho ve vztahu k naplnění daného účelu zpracování vůbec není třeba[91].

Vzniklou újmou, která může být v souvislosti se zpracováním osobních údajů způsobena a v jejímž důsledku může dojít k omezení svobody s nakládáním se souhlasem se zpracováním (udělení či odvolání), se rozumí například situace, kdy odvolání souhlasu se zpracováním vede ke vzniku jakýchkoli nákladů na straně subjektu údajů. V této souvislosti musí být správce vždy schopen prokázat, že při odvolání souhlasu nemůže taková situace nastat.

Konečně pak shora zmíněná granularita představuje situaci, kdy může určitá služba či nabízené plnění zahrnovat zpracování pro několik různých účelů. Jelikož musí být souhlas vždy provázán s konkrétním účelem, je důležité, aby měl subjekt údajů v takových případech vždy možnost si svobodně zvolit účel zpracování, ke kterému svůj souhlas uděluje, a aby nebyl nucen souhlasit s celým souborem účelů zpracování. Konkrétně je pak v pokynu č. 05/2020 Evropského sboru pro ochranu osobních údajů zmíněno, že: *„Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny“*[92]

S ohledem na vše shora uvedené není pochyb o tom, že souhlas se zpracováním údajů je velmi složitým právním titulem pro jejich zpracování, pročež mu byla věnována větší pozornost, než kolik bude tato práce věnovat právním titulům ostatním.

3.1.2. Zpracování pro splnění smlouvy či provedení opatření přijatých před uzavřením smlouvy

[91] Stanovisko pracovní skupiny WP 29 o zpracování údajů na pracovišti č. 2/2017 (WP 249).
[92] Op. cit. Sub 87. 13 s.

Tento právní titul pro zpracování osobních údajů v aplikační praxi nebude činit významné výkladové potíže. Správce osobních údajů je na jeho základě oprávněn ke zpracování osobních údajů v případě, že je takový krok nezbytný k tomu, aby splnil již uzavřenou smlouvu, nebo k tomu, aby provedl opatření související s jejím uzavřením, resp. opatření, která v rámci kontraktačního procesu vedou k uzavření smlouvy.[93] Jinak řečeno se tento právní titul pro zpracování osobních údajů uplatní jak při sjednávání smlouvy, tak při jejím plnění.

Jako nejlepší příklad aplikace tohoto právního titulu v praxi pak poslouží zpracovávání osobních údajů v rámci výběrového řízení u zaměstnavatele, při kterém tento zaměstnavatel zpracovává osobní údaje budoucích potenciálních zaměstnanců.[94] V této souvislosti však zaměstnavatel může pochopitelně zpracovávat pouze takové údaje, které jsou potřebné ke svobodnému a uváženému rozhodnutí o tom, zda s konkrétním zaměstnancem uzavře pracovněprávní poměr, či nikoli. Je tak pochopitelné, že zaměstnavatel bude na základě tohoto právního titulu zpracovávat informace o předchozích pracovních zkušenostech jednotlivých uchazečů. Již ale nebude právně odůvodnitelné, aby zaměstnavatel v případě výběrového řízení zpracovával o potenciálních zaměstnancích například informaci o jejich sexuální orientaci, případně i mimo kategorii zvláštních osobních údajů, například informaci o bankovním spojení (zatímco zpracování takové informace již s přijatým zaměstnancem bude bez pochyby z právního hlediska přijatelné).[95]

3.1.3. Zpracování pro splnění zákonné povinnosti, která se na správce vztahuje

Předně nutno poznamenat, že v souladu s čl. 6. odst. 3 Nařízení může být základ pro zpracování osobních údajů pro splnění zákonné povinnosti stanoven pouze právem Unie, nebo právem členského státu, které se na správce vztahuje, čímž se rozumí, že minimálně účel zpracování osobních údajů musí v tomto případě vycházet přímo ze zákona. Pro titul zpracování pro splnění zákonné povinnosti je typické, že vychází z kogentních právních norem, od kterých nemá správce možnost se za žádných okolností odchýlit. Správce proto nemá na výběr, zda osobní údaje na základě předmětné normy zpracuje, či nikoli – pokud by na výběr měl, musel by k zákonnosti zpracování přistoupit i další titul předpokládaný Nařízením.

[93] Srov. stanovisko pracovní skupiny WP 29 z 9. dubna 2014 č. 6/2014 (WP 217) k pojmu oprávněných zájmů posle Směrnice. 16 a 17 s.
[94] MORÁVEK, J. op. cit. sub 22. 318 s.
[95] Blíže k tomu srov. také ustanovení § 30 zákoníku práce ve spojením s § 316 zákoníku práce.

I tento právní titul zpracování osobních údajů se hojně využívá zejména v pracovním právu, kdy má zaměstnavatel povinnost podle zákoníku práce a souvisejících pracovněprávních a sociálněprávních předpisů zpracovávat o svých zaměstnancích poměrně široké penzum údajů. Tuto povinnost zaměstnavateli stanoví velké množství právních předpisů,[96] přičemž zejména problematické je, že zaměstnavatel musí podle příslušných zákonů zpracovávat různé informace po různě dlouhou dobu po skončení pracovního poměru. Z toho důvodu musí zaměstnavatel těmto zákonným povinnostem věnovat vysokou pozornost.

Pouze pro úplnost lze zmínit, že dotčený právní titul je upraven výslovně také v ZOZOÚ.[97]

3.1.4. Zpracování pro účely ochrany životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby

Podle recitálu (46) Nařízení platí, že: *„Zpracování osobních údajů by mělo být rovněž považováno za zákonné, pokud je nezbytné pro ochranu životně důležitého zájmu subjektu údajů nebo jiné fyzické osoby. Zpracování osobních údajů na základě životně důležitého zájmu jiné fyzické osoby by mělo v zásadě proběhnout pouze tehdy, pokud zjevně nemůže být založeno na jiném právním základě. Některé druhy zpracování mohou sloužit jak důležitým důvodům veřejného zájmu, tak životně důležitým zájmům subjektu údajů, například je-li zpracování nezbytné pro humanitární účely, včetně monitorování epidemií a jejich šíření nebo v naléhavých humanitárních situacích, zejména v případech přírodních a člověkem způsobených katastrof.“*

Z uvedené recitálové definice dotčeného právního titulu zpracování vyplývá, že se v systematice všech právních titulů jedná o jakési *ultima ratio*,[98] neboť *„by mělo* (takové zpracování – pozn. doplněno) *v zásadě proběhnout pouze tehdy, pokud zjevně nemůže být založeno na jiném právním základě“*. Podstatné je, že Nařízení ve srovnání s předchozí úpravou

[96] Příkladem zpracování osobních údajů na základě zákonné povinnosti může být § 35a zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, § 96 zákona č. 187/2006 Sb., o nemocenském pojištění, § 22 c zákona č. 582/1992 Sb., o pojistném na sociálním zabezpečení, nebo § 102 odst. 3 zákona č. 435/2004 Sb., o zaměstnanosti.

[97] Ustanovení § 5 zmíněného zákona říká, že: *„správce oprávněn zpracovávat osobní údaje, pokud je to nezbytné pro splnění povinnosti, která je správci uložena právním předpisem“*

[98] Srov. také stanovisko pracovní skupiny WP 29 z 9. dubna 2014 č. 6/2014 (WP 217) k pojmu oprávněných zájmů posle Směrnice. 20 s.

ve Směrnici a v ZOOÚ již nevyžaduje pro zpracování na základě tohoto právního titulu získat bez zbytečného odkladu dodatečný souhlas subjektu údajů, kterého se zpracování týkalo.[99]

S ohledem na současnou celosvětovou situaci a opět s ohledem na definici obsaženou v recitálu lze dovodit, že toto zpracování bude možné provést například za účelem monitorování epidemie, kdy má předmětné zpracování sloužit vyššímu smyslu a zájem na ochraně osobnosti a soukromí jednotlivce tak ustoupí zájmu na ochraně celospolečenského blaha.

3.1.5. Zpracování pro splnění úkolů prováděných ve veřejném zájmu nebo při výkonu veřejné moci

Tento právní titul pro zpracování se bude vyskytovat v rámci běžně pracovněprávní agendy a pracovněprávních vztahů stejně jaké právní titul předchozí spíše výjimečně. Obecně se totiž bude jednat o takové zpracování osobních údajů, které budou provádět orgány veřejné moci za účelem realizace státní moci a pravomocí svěřených jim zákonem.[100]

Stejně jako pro právní titul zpracování dle čl. 6 odst. 1 písm. c), tedy zpracování pro splnění zákonné povinnosti, která se na správce vztahuje, i zde se uplatní čl. 6 odst. 2 a 3 Nařízení.[101] To znamená, že základ pro zpracování osobních údajů pro splnění úkolů prováděných ve veřejném zájmu nebo při výkonu veřejné moci musí být stanoven pouze právem Evropské unie nebo právem členského státu.

Tento právní titul zpracování osobních údajů se nevztahuje jen na veřejné subjekty, ale mohou jej ke zpracování využívat rovněž subjekty soukromého práva, pokud jsou na základě zákonného podkladu zmocněny k výkonu veřejné moci. Příkladů zpracování na základě čl. 6 odst. 1 písm. e) Nařízení existuje skutečně mnoho, přičemž namátkou lze zmínit například zpracování osobních údajů pro účely přihlášení k trvalému pobytu, pro účely daňové, pro účely veřejné dopravy a užívání motorového vozidla a mnoho dalších.[102]

---

[99] Oproti Směrnici se tento právní titul normovaný Nařízením z popudu Rady vztahuje rovněž na třetí osoby a nikoli pouze na subjekt údajů, jak plyne z BREJCHOVÁ, D. in UŘIČÁŘ, M., RÁMIŠ, V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 6.

[100] Jak ale plyne ze stanoviska pracovní skupiny WP 29 z 9. dubna 2014 č. 6/2014 (WP 217) k pojmu oprávněných zájmů podle Směrnice, na základě tohoto právního titulu může dojít ke zpracování osobních údajů i ze strany soukromých subjektů.

[101] Shodně také např. recitál (45) Nařízení, kde je uvedeno, že: *„Pokud je zpracování prováděno v souladu se zákonnou povinností, která se na správce vztahuje, nebo pokud je zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, mělo by mít toto zpracování základ v právu Unie nebo členského státu.“*

[102] Některým situacím se podrobněji věnuje i samotné Nařízení ve své preambuli srov. např. recitál (55).

3.1.6. Zpracování pro oprávněné zájmy správce či třetí osoby

Podle recitálu (47) Nařízení platí, že: *„Oprávněné zájmy správce, včetně správce, jemuž mohou být osobní údaje poskytnuty, nebo třetí strany se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem.“* a dále, že: *„Existenci oprávněného zájmu je v každém případě třeba pečlivě posoudit, včetně toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít.“* Z uvedeného se podává, že při aplikaci tohoto právního titulu pro zpracování osobních údajů je správce *de facto* vždy povinen provést test proporcionality,[103] v jehož rámci poměří oprávněný zájem svůj či třetí osoby se zájmem subjektu údajů na ochraně jeho soukromí a osobnosti. Pokud v rámci tohoto testu dojde správce k tomu, že se jedná o vhodné, potřebné a přiměřené opatření, bude zpravidla oprávněn ke zpracování osobních údajů přistoupit. Důležité je zmínit, že zpracování na základě tohoto právního titulu slouží ke zpracování pro oprávněné zájmy správce či třetí osoby v obecné rovině, která může například představovat i marketingové záměry.[104]

Jako ideální příklad z praxe pro užití tohoto právního titulu při zpracování osobních údajů poslouží monitoring zaměstnanců ze strany zaměstnavatele za účelem ochrany jeho majetkových zájmu a kontroly, zda zaměstnanci nepoužívají výrobní a pracovní prostředky bez souhlasu zaměstnavatele pro své soukromé účely. Užití tohoto právního titulu je přitom normováno přímo zákonem, konkrétně pak § 316 odst. 1 zákoníku práce.[105] Zákonodárce, vycházeje z definice závislé práce a podmínek, za kterých je vykonávána, normoval odkazovaný právní titul pro zpracování osobních údajů přímo v zákoně primárně proto, že se u zaměstnance, který svou práci vykonává jménem a na náklady zaměstnavatele, dá očekávat, že tak bude činit s užitím prostředků, které nejsou v jeho osobním vlastnictví. Bylo by přitom nedůsledné neumožnit zaměstnavateli alespoň nějakým způsobem kontrolovat, jak jeho zaměstnanci se svěřenými prostředky nakládají. I v rámci tohoto zpracování je však zaměstnavatel povinen provést test proporcionality, aby zjistil, zda je zpracování přiměřené.[106]

---

[103] Srov. například WINTR, J.: *Principy českého ústavního práva.* 2. vydání. Plzeň: nakladatelství Aleš Čeněk. 2013.
[104] Srov. recitál (47) Nařízení.
[105] Srov. blíže například JELÍNEK, T. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář.* 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020. Komentář k § 316.
[106] MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika. 2013. 400 s.

Pokud totiž například zaměstnavatel poskytuje svým zaměstnancům pracovní oděv, lze nakládání s ním kontrolovat jistě méně invazivnějšími prostředky, než je například sledování zaměstnanců pomocí kamerového systému.

Úplným závěrem této části pak lze zmínit pozitivní posun Nařízení oproti dřívější úpravě a jejímu výkladu, který je reprezentovaný recitálem (48) Nařízení.[107] Tento recitál totiž automaticky počítá s tím, že oprávněný zájem vzniká, resp. ho mohou mít, správci, kteří jsou součástí skupiny[108] podniků nebo institucí přidruženým k ústřednímu orgánu, a to konkrétně na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců.[109]

3.2. Ke zpracování zvláštních kategorií osobních údajů

Ještě než budou v práci detailněji rozebrány i ostatní povinnosti správců údajů zmíněné v úvodu této kapitoly, bude v ní v krátkosti věnována pozornost i právním titulům pro zpracování zvláštních kategorií osobních údajů, které jsou oproti právním titulům zpracování osobních údajů dle čl. 6 odst. 1 Nařízení modifikovány.

Prolomení obecného zákazu zpracování zvláštních kategorií osobních údajů lze dosáhnout desíti různými způsoby (včetně udělení souhlasu, kterému však byla věnována pozornost již výše), i když s jejich užitím by mělo vždy být nakládáno restriktivním způsobem.[110] Těmito jsou:

(i) Zpracování pro účely plnění povinností a výkon zvláštních práv v oblasti pracovního práva a práva sociálního zabezpečení a sociální ochrany – Takové zpracování je umožněno pouze za předpokladu, že je povoleno právem Evropské unie nebo členského státu či kolektivní dohodou podle práva členského státu, které vhodně zaručuje ochranu základních práv a zájmů subjektu údajů. Typickým příkladem zpracování takového citlivého údaje jsou situace, kdy zaměstnavatel vede informaci o tom, že je jeho zaměstnanec odborově

[107] K pozitivním důsledkům této změny a zlepšení právního stavu s ní související srov. MORÁVEK, J. op. cit. sub 22. 197 a 198 s.
[108] Typickým příkladem takového jednání v rámci skupiny podniků je koncern tak, jak je definován v ustanovení § 79 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích).
[109] I v případě předávání informací v rámci skupiny bude nutné vždy provést balanční test s ohledem na zásadu minimalizace údajů podle čl. 5 odst. 1 písm. c) Nařízení, jak plyne z BREJCHOVÁ, D. in UŘIČÁŘ, M, RÁMIŠ V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 6.
[110] Ibid. Komentář k čl. 9.

organizovaný a že je například i členem orgánu odborové organizace (srov. například § 203 zákoníku práce či § 61 odst. 2 zákoníku práce);

(ii) Zpracování pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, je-li tento subjekt právně nezpůsobilý k udělení souhlasu – Pro podrobnější výklad vizte kapitolu 3.1.4 výše;

(iii) Zpracování prováděné v rámci oprávněných činností a s potřebnými zárukami například nadací, sdružením nebo jiným neziskovým subjektem sledující politické, filosofické, náboženské či odborové cíle, pokud se toto zpracování vztahuje na současné či bývalé členy – Tento speciální právní titul je zohledněn již v recitálu (51) Nařízení, kde je uvedeno, že se uplatní, pokud je zpracování prováděno v průběhu oprávněných činností některých sdružení či nadací, jejichž cílem je umožnit výkon základních svobod. Z toho se podává, že tato výjimka se uplatní na podobné organizace především ve vztahu ke zpracovávání informací o členství, kdy například určitý počet členů může mít vliv na oprávnění předmětné organizace;

(iv) Zpracování údajů zjevně zveřejněných subjektem údajů – tento právní titul zpracování je hojně využívaný zejména v online prostředí, kdy například pro účely oslovování potenciálních zákazníků využívají správci kontaktní údaje subjektu údajů na jejich internetových stránkách, kde byly tyto zveřejněny;

(v) Zpracování pro určení, výkon nebo obhajobu právních nároků – k tomu vizte kapitola 3.1.6 výše; a

(vi) Zpracování, které je nezbytné z důvodů uvedených ve veřejném zájmu dle čl. 9 odst. 2 písm. g), i) a j) Nařízení či pro účely preventivního nebo pracovního lékařství – zpracování zvláštních kategorií osobních údajů je rovněž umožněno na základě hned několika rovin veřejného zájmu. Mezi ty patří zájem v oblasti veřejného zdraví, zájem v oblasti archivace s ohledem na vědecké a historické badání a pro statistické účely a zájem (resp. významný důvod veřejného zájmu) existující na základě práva Evropské unie nebo členského státu. U těchto právních titulů je pak Nařízením vždy explicitně zmíněno, že je lze uplatnit jen za předpokladu, že jsou přiměřené sledovanému cíli a dodržují podstatu práva

na ochranu údajů, přičemž musí poskytovat vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

Pro účely této práce je zpracování zvláštních kategorií osobních údajů podstatné především proto, že se bude v kapitole šesté věnovat otázce biometrických údajů, a to zejména s ohledem na stále se zvyšující digitalizaci a elektronizaci veřejného i soukromého prostoru.

3.3. Povinnost k účelovému omezení a minimalizaci údajů

Každý správce údajů je povinen před zpracováním osobních údajů stanovit účel, pro který dotčené osobní údaje zpracovává. Tyto údaje dále nesmí být zpracovávány způsobem, který je s tímto účelem/účely neslučitelný. Zároveň musí být při zpracování osobních údajů za stanoveným účelem dodržena povinnost jejich minimalizace, tedy že správce musí osobní údaje zpracovávat vždy přiměřeně a pouze v nezbytné míře.[111] Jelikož jsou obě dvě tyto povinnosti co do hypotézy právní normy velmi obdobné a vzájemně se překrývají, bude o nich v této podkapitole pojednáno společně.

Jak naznačeno shora, obě povinnosti v sobě skrývají jednak nutnost zpracování osobních údajů pouze v nezbytně nutném rozsahu ve vztahu ke sledovanému účelu, jednak zákaz sdružování, kombinace či jakéhokoli spojování údajů, které byly získány k rozdílným účelům (v tom je zahrnut také zákaz zpracování osobních údajů za jiným účelem, než k jakému byly tyto osobní údaje původně zpracovány). V ZOOÚ byly tyto zásady vyjádřeny *de iure* v ustanovení § 5 odst. 1 písm. a), d), f), g) a h) kde bylo normováno, že správce je povinen (i) stanovit účel, pro který mají být osobní údaje zpracovány, (ii) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a rozsahu nezbytnému pro naplnění stanoveného účelu, (iii) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, (iv) shromažďovat osobní údaje pouze otevřeně a (v) nesdružovat osobní údaje, které byly získány k rozdílným účelům. Směrnice pak povinnosti správce osobních údajů a tím pádem i projevy zmíněných zásad normovala v čl. 6.

Kritérium přiměřenosti zpracování osobních údajů je nezbytné posuzovat vždy ve vztahu ke stanovenému účelu zpracování, protože každému účelu pro zpracování musí

[111] K tomu, jak by měl každý správce osobních údajů vždy poměřovat všechny způsoby zpracování a zvolit ten nejméně invazivní, vizte např. stanovisko ÚOOÚ č. 6/2009: *Ochrana soukromí při zpracování osobních údajů*. Listopad 2009. Aktualizováno v únoru 2014.

pochopitelně odpovídat i jiný rozsah zpracování.[112] Z toho důvodu by měl být správce schopen posoudit již před samotným zpracováním osobních údajů, v jakém rozsahu tyto bude muset zpracovávat, aby bylo dosaženo stanoveného účelu, pročež musí být tato povinnost řádně plněna již ve fázi shromažďování osobních údajů jako v první fázi jejich zpracování. Tuto povinnost správce osobních údajů lze souhrnně označit jako tzv. záměrnou a standardní ochranu osobních údajů, což je koncept, jehož obsahem je povinnost správce údajů jak v době nastavování parametrů pro nové zpracování osobních údajů, tak i v jeho průběhu, aplikovat technická a organizační opatření k zajištění toho, aby zpracování osobních údajů probíhalo v souladu s obecným nařízením a aby byla ochráněna práva dotčených osob.[113]

Rozsah zpracování osobních údajů může být přitom určen dvěma způsoby. Prvním z nich je, že rozsah zpracování vyplývá přímo z mandatorních ustanovení zákona. To bude platit například při zpracovávání osobních údajů zaměstnanců pro účely obligatorních zákonných odvodů, přičemž by naplnění kritéria přiměřenosti a jeho hodnocení nemělo v praxi činit větší potíže. Druhým způsobem je vymezení rozsahu zpracování přímo na základě rozhodnutí správce osobních údajů. V této souvislosti musí správci myslet především na to, že porušení povinnosti přiměřenosti, resp. účelového omezení, nelze exkulpovat tím, že by ke zpracování osobních údajů ve větším rozsahu získal správce souhlas subjektu údajů.

Nutno také podotknout, že princip a kritérium přiměřenosti má své projevy přímo i v zákoníku práce. Především pak § 316 explicitně zmiňuje, že zaměstnavatel může s osobními údaji ve vztahu ke sledovanému účelu nakládat pouze přiměřeně, přičemž vyžadování určitých informací přímo vylučuje. Obdobné projevy lze dále nalézt například v § 30 či § 312 zákoníku práce.[114] Závěrem lze dodat, že dosažení tohoto principu při zpracování přitom úzce souvisí s aplikací čl. 25 Nařízení, které je projevem shora zmíněného konceptu záměrné a standardní ochrany osobních údajů.[115]

---

[112] NONNEMANN, F. in KUČEROVÁ, A., NOVÁKOVA, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2012. Komentář k § 4.

[113] NONNEMANN, F. *Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů?* [dostupné online na epravo.cz]. Epravo. 2018.

[114] Ustanovení § 30 odst. 2 zákoníku práce například říká, že: „*Zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy*.“ Ustanovení § 312 odst. 1 zase, že: „*Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3.“* Dále k tomu také srov. MORÁVEK, J. op. cit. sub 22. 202 s.

[115] Čl. 25 Nařízení stanoví povinnost správcům osobních údajů zavést vhodná technická a organizační opatření, a to jak v době určení prostředků zpracování, tak přímo v době zpracování samotného.

Ve vztahu ke kritériu účelového omezení platí, že určí-li správce osobních údajů účel jejich zpracování, dochází k tomu, že na straně subjektů údajů vznikne legitimní očekávání, že získané údaje boudou požity právě a výlučně k naplnění předem stanoveného účelu[116], a nebudou proto kombinovány, přiřazovány či zaměňovány k osobním údajům, jež byly shromážděny a zpracovány k naplnění naprosto odlišného cíle. Možnost porušit toto pravidlo a sdružit údaje za jiným účelem, než pro který byly původně zpracovány, správci svědčí pouze tehdy, pokud k tomu má právními předpisy stanovený důvod. Odborná literatura v této souvislosti uvádí, že mohou nastat dvě situace, ve kterých může správce takto postupovat.

Zaprvé je možné tak učinit, pokud k tomu správce osobních údajů získá dodatečný souhlas subjektu údajů (za předpokladu, že zůstane splněno kritérium přiměřenosti), jedná-li se o splnění zákonné povinnosti. Druhým případem je, dojde-li k naplnění testu slučitelnosti účelů, jak je koncipován v čl. 6 odst. 4 Nařízení.[117] Splnění testu slučitelnosti přitom musí vycházet buďto přímo ze zákona,[118] nebo jeho splnění musí posuzovat sám správce osobních údajů, a to vždy s přihlédnutím k testu proporcionality. Pro úplnost je nutné upozornit, že speciální pravidlo ke slučitelnosti účelů normuje ještě také ZOZOÚ, a to konkrétně v § 6, kde je stanoveno, že správce není povinen při zajišťování chráněného zájmu posuzovat před zpracováním osobních údajů k jinému účelu, než za jakým mělo být původně zpracováváno, jejich slučitelnost, je-li takové zpracování nezbytné pro splnění (i) zákonné povinnosti, která je správci uložena, nebo (ii) úkolu ve veřejném zájmu stanoveného právním předpisem nebo při výkonu veřejné moci, kterým je správce pověřen.

Z hlediska zákonné úpravy pracovního práva lze jako příklad, kdy je test slučitelnosti jednoznačně naplněn, použít situaci, kdy zaměstnavatel nejdříve shromáždí osobní údaje určitého subjektu údajů v rámci výběrového řízení na konkrétní pracovní pozici, přičemž jakmile danou osobu přijme do pracovněprávního poměru, sloučí takto získané údaje s nově získanými tak, jak je musí mít shromážděné a zpracované pro účely existence pracovněprávního vztahu.

---

[116] Tento účel je přitom nutné stanovit nejpozději při shromáždění osobních údajů, srov. NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer, 2017. 108 s.

[117] Podle zmíněného čl. Nařízení platí, že správce musí při zpracování pro jiný účel (pokud nevyplývá ze souhlasu subjektu údajů či přiměřeného a nutného opatření založeného právem Evropské unie nebo členského státu) zohlednit vazbu mezi účelem původního zpracování a nového plánovaného účelu, okolnosti, za kterých byly informace zpracovány, povahu osobních údajů, možné důsledky dalšího zamýšleného zpracování a existenci vhodný záruk včetně šifrování a pseudonymizace.

[118] Srov. například ustanovení § 6 zákona č. 435/2004 Sb., o zaměstnanosti.

Ke splnění těchto povinností správce osobních údajů tak obecně lze říci, že se jedná o záruku subjektu údajů v tom smyslu, že jejich osobní údaje nebudou z žádného hlediska zpracovávány v širším rozsahu, než jak je to pro správce nezbytně nutné. To vše bez ohledu na to, zda zpracováním správce plní zákonnou povinnost, nebo údaje zpracovává ve svůj vlastní prospěch, jak je tomu například u účelů marketingových. Ať už zpracování ale probíhá za jakýmkoli účelem, správce osobních údajů pro naplnění povinnosti účelového omezení musí pamatovat na to, že osobní údaje je možno vždy zpracovat jen pro určité, výslovně vyjádřené a legitimní účely.[119]

3.4. Povinnost k přesnosti údajů

Ve vztahu k této povinnosti správce údajů Nařízení stanoví, že musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.[120] Podle odborné literatury jsou typickým příkladem, kde je vyžadována dostatečná přesnost zpracovávání osobních údajů, pracovněprávní vztahy, ve kterých je naprosto běžné, že jako opatření vedoucí k uchování přesných údajů zaměstnavatelé mohou dát do pracovní smlouvy povinnost zaměstnance je bezodkladně informovat o jakékoli změně zpracovávaných osobních údajů.[121]

Základem této povinnosti při zpracování osobních údajů je premisa, že zpracování nepřesných údajů může mít obdobně negativní důsledky, jako když správce porušuje povinnost minimalizace osobních údajů, protože i nepřesně zpracované osobní údaje mohou vést k právním jednáním, která by se byla bývala nikdy nestala, pokud by údaje byly přesné.

Typickým příkladem takové situace může být schválení úvěru subjektu údajů na základě informací o jeho majetkových poměrech, které nejsou správné. Aby se podobně negativním důsledkům při zpracování osobních údajů předcházelo, je správce povinen v první řadě všechny zpracovávané osobní údaje pravidelně aktualizovat. Není-li to v dané situaci možné a existuje-li zde podezření o nesprávnosti, resp. nepřesnosti zpracovávaných údajů, je správce údajů povinen osobní údaje bez dalšího zlikvidovat. Podstatné rovněž je, že správce údajů vždy musí zpracovávat údaje komplexně, má-li takovou povinnost ze zákona. To jinými slovy znamená, že pokud správce má na základě právních předpisů o sociálním a zdravotním pojištění

[119] Tyto tři základní parametry zásady účelového omezení plynou ze stanoviska pracovní skupiny WP 29 k účelovému omezení ze dne 2. dubna 2013 č. 3/2013 (WP203).
[120] Srov. čl. 5 odst. 1 písm. d) Nařízení.
[121] MORÁVEK, J. op. cit. sub 22. 203 s.

povinnost zpracovávat určité penzum osobních údajů o svých zaměstnancích a nečiní tak, jsou údaje nepřesné a dochází k porušení popsané povinnosti i v takovém případě.

V souvislosti s povinností správce osobních údajů zpracovávat tyto přesně pak úzce souvisí i určitá oprávnění subjektu údajů, kterým se bude podrobněji věnovat následující kapitola. V úplném závěru této podkapitoly je důležité zmínit, že přesností se ve smyslu Nařízení v žádném případě nemyslí pravdivost a 100% objektivita zpracovávaných osobních údajů. Ty musí být totiž správné pouze za vymezeným účelem, což ale může v některých situacích zároveň odůvodňovat fiktivnost zpracovaných údajů.

3.5. Povinnost k omezení uložení

Osobní údaje lze zpracovávat a smějí být uloženy pouze ve formě umožňující identifikaci subjektu údajů jen po takovou dobu, která je nezbytně nutná pro naplnění účelu, pro který jsou osobní údaje zpracovávány.[122]

Již při pohledu na ostatní povinnosti správců údajů popsané výše v této kapitole je zřejmé, že hlavní cíl celé právní úpravy ochrany osobních údajů (a tedy i Nařízení) je nastavit její pravidla tak, aby nebylo nic v rámci zpracování činěno ve větším (ale ani v menším) rozsahu, než je nezbytně nutné. Z Nařízení tak plynou povinnosti, jakože správce musí osobní údaje zpracovávat jen v určité kvalitě, může je zpracovávat jen za určitým účelem, který nemůže svévolně měnit, musí je v určité míře kvality ochraňovat atp. Stejné pravidlo se přitom použije také na dobu, po kterou je správce oprávněn osobní údaje zpracovávat. Jak ale správně uvádí například Morávek,[123] platí, že správce má sice povinnost zpracovávat osobní údaje subjektu údajů jen po určitou dobu v souladu se stanoveným účelem, přičemž by se ale neměl ukvapovat ani s jejich likvidací.

To platí především v situaci, kdy může dojít k tzv. slučitelnosti účelů zpracování, kdy jsou údaje nejdříve zpracovávány za jedním účelem a na základě jednoho právního titulu a následně je může správce zpracovávat i dále v důsledku automatické změny účelu i právního titulu užívání. Již jednou popsaný případ, kdy bude test slučitelnosti naplněn, je situace, když zaměstnavatel zpracovává údaje kandidáta na určitou pracovní pozici, které si následně ponechá a i nadále je ukládá v případě, že danou osobu na pracovní místo zaměstná. V této souvislosti

[122] Srov čl. 5 odst. 1 písm. e) Nařízení
[123] MORÁVEK, J. op. cit. sub 22. 205 s.

mnohem častější však bude z praktického hlediska případ, kdy si správce osobních údajů ponechává informace například za účelem plnění smlouvy či zákonných povinností po dobu existence smluvního vztahu, ale následně ještě i tři roky po jeho skončení, a to za účelem usnadnění své důkazní situace v případě potenciálního budoucího sporu. Tj. situace, kdy si správce osobních údajů tyto údaje ponechá na základě právního titulu ochrany svých oprávněných zájmů, neboť ví, že kdyby jej subjekt údajů v budoucnu v souvislosti s daným právním vztahem zažaloval a správce se osobních údajů zbavil, neunesl by v daném sporu své důkazní břemeno.

Ať už se správce v souvislosti s dobou zpracování osobních údajů rozhodne jakkoli, musí však pamatovat na to, že se jedná jen a pouze o jeho odpovědnost. Posouzení doby zpracování je jednoduché v případě, kdy zákon přímo stanoví, po jak dlouhou dobu správce musí předmětné údaje zpracovávat.[124] Složitější je dané posouzení zpravidla za předpokladu, kdy si správce údaje ponechává a nadále je zpracovává právě především za účelem ochrany svých vlastních zájmů. Této okolnosti totiž bez dalšího nelze zneužívat a doba uchování osobních údajů nesmí být nikdy delší, než vyžaduje zpracováním sledovaný účel (ve shora popsaném případě se tak typicky bude jedna právě o tři roky z důvodu běhu promlčecích lhůt k uplatnění nároku v rámci soudního řízení). V této souvislosti je však třeba zmínit, že podle názoru ÚOOÚ není odkaz na zákonné lhůty vhodný tam, kde není důvodné žádný soudní spor předpokládat, resp. tam, kde soudní spor, pro který si správce údaje ponechával, již skončil.[125] Stejně tak platí, že doba zpracování nesmí být stanovena příliš neurčitě, jelikož ve všech případech dojde k objektivnímu posouzení, zda taková doba stanovená správcem skutečně odpovídá jakýmkoli oprávněným zájmům.[126]

3.6. Povinnost k integritě a důvěrnosti

Poslední zásada explicitně zmíněná v čl. 5 Nařízení projevující se rovněž do povinností správce osobních údajů je zásada integrity, důvěrností a standardní ochrany.[127]

[124] Příkladem zpracování osobních údajů na základě zákonné povinnosti může být § 35a zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, § 96 zákona č. 187/2006 Sb., o nemocenském pojištění, § 22 c zákona č. 582/1992 Sb., o pojistném na sociálním zabezpečení, nebo § 102 odst. 3 zákona č. 435/2004 Sb., o zaměstnanosti.
[125] Rozhodnutí ÚOOÚ z 21. března 2013, č. j. SKO-2077/07.
[126] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer. 2017. 114 s.
[127] Srov. čl. 5 odst. 1 písm. f) Nařízení.

Tato povinnost neříká nic jiného, než že je správce osobních údajů povinen tyto zabezpečovat takovým způsobem, aby nemohlo docházet k jejich porušení a jakémukoli zneužití. I plnění této povinnosti vychází ze shora zmíněného principu záměrné a standardní ochrany.[128][129] Tento princip nezahrnuje pouze úpravu zabezpečení osobních údajů, ale rovněž se váže na zásadu odpovědnosti správce osobních údajů, která nastává v případě úniku osobních údajů při jejich nedostatečném zabezpečení. Správce osobních údajů je v této souvislosti povinen přijmout vhodná technická a organizační opatření, která povedou ke garanci naplňování této zákonné povinnosti.

Ve vztahu k dotčené povinnosti správce osobních údajů je podstatné, že se jemu (resp. pověřenému zpracovateli) ukládá, aby ji dodržoval v rámci celého procesu zpracování a aby ideálně ještě před samotným započetím se zpracováním měl jasně rozmyšleno, jaká technická a organizační opatření budou v daném případě zpracování dostatečná. Cílem této povinnosti, tedy hledání těch nejlepších opatření ještě před samotným zpracováním, je dosažení dostatečné garance bránící neoprávněnému přístupu k osobním údajům.[130] Evropský zákonodárce však při tvorbě Nařízení nezatížil touto obecnou obezřetností pouze správce či zpracovatele, ale dokonce i výrobce a poskytovatele zejména té technické stránky opatření vedoucích k ochraně osobních údajů, když v recitálu (78) Nařízení stanovil, že: *„Pokud jde o vývoj, koncepci, výběr a používání aplikací, služeb a produktů, které jsou založeny na zpracování osobních údajů nebo osobní údaje za účelem plnění svých funkcí zpracovávají, je třeba zhotovitele těchto produktů, služeb a aplikací vybízet k tomu, aby při vývoji a koncipování těchto produktů, služeb a aplikací zohledňovali právo na ochranu údajů a brali náležitý ohled na stav techniky s cílem zajistit, aby správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů.“*

Odborná literatura k této povinnosti správce uvádí, že je správce, resp. zpracovatel osobních údajů, při snaze dodržet povinnost důvěrnosti a integrity zejména povinen zajistit složku (i) personální, (ii) výpočetní techniky a (iii) prostorovou.[131]

[128] Tento princip se mj. váže na zásadu odpovědnosti, ze které vyplývá povinnost správce být schopen prokázat řádné plnění jednotlivých povinností dle čl. 5 Nařízení. Srov. k tomu také MORÁVEK, J. op. cit. sub 22. 209 s., nebo NONNEMANN, F. op cit. sub 113.
[129] Nepřímo byl tento princip obsažen už také ve Směrnici, konkrétně v recitálu (46) a čl. 17.
[130] K jejímu naplnění se proto váže spoustu dalších ustanovení Nařízení, jako např. povinnost oznamování a ohlašování dle čl. 33 a 34 Nařízení nebo např. vyhotovování záznamů o činnostech zpracování dle čl. 30 Nařízení.
[131] MORÁVEK, J. op. cit. sub 22. 211 s

To jinými slovy znamená, že správce osobních údajů musí v souladu s organizačně-technickým zabezpečením zpracování osobních údajů vždy jasně určit, které osoby budou mít k osobním údajům přístup, a jak s nimi tyto jednotlivé osoby budou moci nakládat. V souvislosti s tím je rovněž nutné zajistit, aby se osobní údaje, resp. přístup k nim nacházel v místech, které jsou pod dostatečnou ochranou, a na které se vztahují striktní pravidla ohledně přístupu a možnosti tyto prostory používat. Konečně pak hledisko výpočetní techniky vycházeje z hlediska personálního a prostorového musí být zejména v dnešní době moderních technologií zajištěno dostatečnými opatřeními. Danou výpočetní techniku by tak měly používat pouze osoby znalé oboru, které jsou v jejím užívání řádně proškolené, neměla by být bez dalšího přístupná všem osobám u správce či zpracovatele osobních údajů a její stupeň ochrany by měl odpovídat technologickému vývoji a pokroku dnešní doby.

Jen pokud správce osobních údajů splní řádně všechny tyto dílčí povinnosti, je zásada důvěrnosti a integrity ochrany osobních údajů řádně naplněna. Jak přitom plyne z komentářové literatury, platí, že: *„Zásada integrity a důvěrnosti tak požaduje, aby byly údaje zpracovávány pouze tak, aby bylo zajištěno zabezpečení osobních údajů. Stejně jako ostatní zásady se zásada důvěrnosti a integrity aplikuje na celý proces zpracování osobních údajů, zahrnuje tak všechny fáze zpracování osobních údajů od shromáždění, ukládání, využití, přenosu až po jejich likvidaci.“*[132]

3.7. Další povinnosti správce osobních údajů

Nařízení pochopitelně upravuje i další povinnosti správců osobních údajů, které však nejsou vyjmenovány v čl. 5 Nařízení upravujícím základní principy zpracování osobních údajů, resp. z něj automaticky implicitně nevyplývají. Jedná se především o povinnosti související s posouzením vlivu na ochranu osobních údajů a s oznamováním a ohlašováním porušení zabezpečení osobních údajů.[133]

Posuzování vlivu na ochranu osobních údajů coby povinnost správce, resp. zpracovatele osobních údajů, velmi úzce souvisí se shora uvedenými povinnostmi vázanými ke garanci integrity a důvěrnosti. Posouzení vlivu je totiž správce povinen provést v situaci, kdy při zpracování dochází k využití nových technologií, jejichž použití může s ohledem na rozsah

[132] RÁMIŠ, V. in UŘIČÁŘ, M, RÁMIŠ V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 5.
[133] Primárně jde tedy o oddíl 3 Nařízení a články 33 a 34 Nařízení.

a účel zpracování značně zvýšit riziko pro práva a svobody subjektu údajů.[134] Posouzení vlivu na ochranu osobních údajů musí přitom správce provést zejména ve třech konkrétních situacích, a sice:

(i) Při systematickém a rozsáhlém vyhodnocování osobních aspektů subjektu údajů, které je založeno na automatizovaném zpracování a profilování, z něhož vycházejí rozhodnutí mající vliv přímo na subjekty údajů;

(ii) Při rozsáhlém zpracování zvláštní kategorie osobních údajů; a

(iii) Při rozsáhlém a systematickém monitorování veřejně přístupných prostorů.[135]

Uvedené však nic nemění na závěru, že správce osobních údajů je vždy povinen zajistit, aby nedocházelo při zpracování osobních údajů k jejich úniku, a i když posouzení vlivu ve smyslu čl. 35 Nařízení míří především na shora popsané situace, správce musí mít tuto povinnost na paměti vždy bez ohledu na způsob a rozsah zpracování.

Čl. 35 Nařízení dále dává v odst. 7 správci osobních údajů návod, co musí konkrétně jeho posouzení zahrnovat. Jedná se přitom o (i) systematický popis zamýšlených operací zpracování a účelu zpracování, (ii) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu zpracování, (iii) posouzení rizik pro práva a svobody subjektů údajů a (iv) plánovaná opatření řešení rizik, včetně záruk, bezpečnostních opatření a mechanismů k zabránění porušení ochrany osobních údajů. Jako určité vodítko pro správce osobních údajů, kdy je nutné posouzení vlivu provést kromě čl. 35 Nařízení rovněž slouží speciální metodika pracovní skupiny WP 29, která obsahuje devět kritérií rizikovosti, kdy při naplnění alespoň dvou z nich správce většinou musí posouzení provést.[136] Obdobný dokument vydal rovněž ÚOOÚ, který těchto kritérií pro změnu stanovil ve svém dokumentu deset. Rozdělil je do tří samostatných kategorií závažnosti.[137] I v tom je přitom návodně popsáno, při splnění jakých z nich by správce posouzení vlivu měl provést.

[134] Pokyny pracovní skupiny WP29 pro posouzení vlivu na ochranu údajů a stanovení, zda *„je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“* pro účely Nařízení ze dne 4. dubna 2017 ve znění z 4. října 2017 č. WP 248 rev. 01. 12 s.
[135] Srov čl. 35 odst. 3 Nařízení a tam uvedený demonstrativní výčet.
[136] Op. cit. sub 134.
[137] Dokument ÚOOÚ k povinnosti správců provádět posouzení vlivu na ochranu osobních údajů. Publikováno dne 8. února 2019.

Závěrem lze zmínit, že na povinnost k posouzení vlivu je velmi úzce navázán i následující čl. 36 Nařízení, jenž stanoví správci další povinnost související s touto problematikou, a sice povinnost předchozí konzultace s dozorovým úřadem (v České republice ÚOOÚ). To musí správce učinit, pokud při posouzení vlivu dojde k závěru, že zde existuje vysoké riziko porušení práv subjektu údajů za předpokladu, že by nedošlo k přijetí konkrétních opatření.[138]

Další významnou povinnost správce osobních údajů normují čl. 13 a čl. 14 Nařízení. Tyto dva články upravují povinnosti správce ohledně informací, které je správce povinen poskytovat subjektu údajů v případě, že jsou osobní údaje získávány přímo od něj, a v případě, že osobní údaje nebyly získány od subjektu údajů. Tato povinnost je velmi podstatná zejména z toho důvodu, že zakládá zákonnost celého zpracování, kdy pouze při jejím naplnění získává subjekt údajů všechny informace, které potřebuje k tomu, aby mohla být v úplnosti naplněna jeho práva.

Některé z poskytovaných informací na sebe přitom navazují další povinnosti správce – když se správci například přikazuje poskytnout informace o pověřenci pro ochranu osobních údajů, odráží to i povinnost tohoto pověřence jmenovat;[139] když se správci přikazuje informovat subjekt údajů o příjemcích zpracovaných údajů, zahrnuje to v sobě i povinnost správce udržovat aktualizovaný seznam všech těchto příjemců; a konečně když se správci přikazuje poskytnout subjektu údajů informaci o tom, zda budou jeho osobní údaje předávány do třetích zemí, musí správce osobních údajů plnit všechny povinností s tímto spojené.[140]

Poslední povinnost správce osobních údajů, které bude v této práci věnována větší pozornost, je povinnost oznamování a ohlašování porušení zabezpečení.[141][142] Co se rozumí porušením, je definováno přímo v čl. 4 Nařízení, který uvádí, že taková situace představuje porušení zabezpečení, jež vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Bližší specifikaci případů porušení zabezpečení osobních

[138] Z čl. 36 Nařízení plyne, že správce osobních údajů má v některých situacích fakultativní možnost konzultace (srov. odst. 1 dotčeného čl.) a v některých situacích obligatorní povinnost konzultace (srov. odst. 5 dotčeného čl.).
[139] Srov čl. 37 Nařízení nazvaný „*jmenování pověřence pro ochranu osobních údajů*".
[140] Srov. především čl. 44 a násl. Nařízení.
[141] Srov. čl. 33 a čl. 34 Nařízení.
[142] Jak přitom plyne z komentářové literatury, o těchto dvou povinnostech je správné pojednat společně, neboť i odborné dokumenty od pracovní skupiny WP 29, resp. od Evropského sboru pro ochranu osobních údajů tak většinou činí: srov. UŘIČÁŘ, M. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 33 Nařízení.

údajů, ke kterým se vztahuje povinnost správce tyto ohlašovat, pak nabízí pracovní skupina WP 29. Ta rozděluje případy porušení do tří samostatných kategorií, kterými jsou (i) porušení důvěrnosti – situace, kdy dojde k neoprávněnému nebo náhodnému poskytnutí nebo zpřístupnění osobních údajů, (ii) porušení dostupnosti – situace, kdy dojde k náhodné nebo neoprávněné ztrátě přístupu nebo zničení osobních údajů a (iii) porušení integrity – situace, kdy dojde k neoprávněnému nebo náhodnému pozměnění zpracovaných osobních údajů.[143] Z popsaných okolností možného porušení ochrany osobních údajů je zřejmé, že i tato povinnost správce (stejně jako posuzování vlivu na ochranu popsané shora) je velmi úzce spojena se zásadou (resp. povinností) důvěrnosti a integrity zpracování osobních údajů.

Uvedené plyne již jen z toho, že ohlašování a oznamování případů porušení zabezpečení osobních údajů je normováno v čl. 33 a čl. 34 Nařízení, přičemž čl. 32 a násl. Nařízení upravují právě oblast zabezpečení osobních údajů obecně. Základní povinností správce, jež má předcházet povinnosti ohlašování a oznamování, proto pochopitelně je povinnost provést spolu se zpracovatelem vhodná technická a organizační opatření za účelem zajištění zabezpečení úrovni odpovídající danému riziku, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.[144]

Rozdíl mezi ohlášením a oznámením o porušení zabezpečení osobních údajů spočívá v tom, jaká je intenzita daného případu porušení. V případě jakéhokoli porušení (bez ohledu na intenzitu zásahu do práv subjektů údajů) je správce vždy povinen tento incident ohlásit. Nařízení přitom stanoví, že by tak měl učinit do 72 hodin od okamžiku, kdy se o takovém porušení dozvěděl, a to dozorovému orgánu dle čl. 55 Nařízení – je-li toto ohlášení učiněno později, musí společně s ním správce dozorovému orgánu sdělit důvody, proč nebylo možné jej provést ve stanoveném časovém úseku. Článek 33 odst. 3 Nařízení stanoví, jaké minimální informace musí ohlášení dozorovému orgánu obsahovat,[145] přičemž nedílnou součástí ohlášení učiněného po více než 72 hodinách od daného incidentu je právě legitimní zdůvodnění tohoto opoždění.

[143] Doporučení pracovní skupiny WP 29 z 3. října 2017 – Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679. 6 s.
[144] Tak musí správce společně se zpracovatelem podle čl. 32 Nařízení učinit případně včetně šifrování a pseudonymizace, zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systému zpracování, obnovení dostupnosti údajů v případě jakéhokoli incidentu a vytvoření procesu pravidelného testování, který bude zkoumat účinnost zavedených technických a organizačních opatření.
[145] Srov čl. 33 odst. 3 Nařízení

V případě, že je pravděpodobné, že bude mít porušení zabezpečení osobních údajů za následek vysoké riziko pro práva a svobody subjektů údajů, musí tuto skutečnost správce oznámit bez zbytečného odkladu, a to právě těmto subjektům údajů. Nařízení nestanovuje pro oznámení subjektům údajů žádnou rámcovou lhůtu, jako je tomu v případě ohlášení dle čl. 33 Nařízení, ale vzhledem k tomu, že se obecně jedná o více intenzivní zásah do práv subjektů údajů a že se musí oznamovat nejen dozorovému orgánu, ale přímo těmto subjektům, mělo by oznámení být provedeno vždy ještě před samotným ohlášením – v tomto kontextu si lze představit, že zdůvodnění pro provedení ohlášení až po stanovených 72 hodinách bude právě situace, kdy správce předně oznamoval ohrožení práv a svobod subjektů údajů těmto subjektům, čímž sledoval důležitější zájem chráněný Nařízením. Jako příklad takového porušení zabezpečení, které by měl správce bezodkladně oznámit subjektům údajů, je ztráta zdravotnické dokumentace, kdy je pro další léčbu subjektů údajů nezbytné znát předchozí léčebný postup, podávané léky, anamnézu, správou diagnostiku atd.[146]

Vzhledem k tomu, že oznámení porušení zabezpečení se neprovádí vůči dozorovému orgánu, který pracuje s odborným aparátem v oblasti ochrany osobních údajů, ale vůči konkrétním subjektům údajů, kteří budou zpravidla právními laiky, musí být oznámení co možná nejjednodušší a jeho obsah musí být adresátovi srozumitelný.[147] Zároveň platí, že oznámení musí obsahovat alespoň následující informace – (i) popis povahy porušení, (ii) jméno a kontakt na pověřence pro ochranu osobních údajů či jiné kontaktní místo, (iii) popis pravděpodobných důsledku porušení a (iv) popis přijatých opatření k nápravě.[148] Nařízení rovněž vymezuje situace, za kterých nemusí být oznámení ze strany správce učiněno.[149]

V této souvislosti stojí za zmínku, že pokud by oznámení vyžadovalo ze strany správce nepřiměřené úsilí, musí stejně správce oznámení učinit, a to alespoň stejně efektivním způsobem pomocí veřejného oznámení nebo jiného potřebného opatření. Jinými slovy Nařízení v této rovině rovněž pamatuje na situace, kdy dojde k porušení zabezpečení vyžadujícímu oznámení ve vztahu k enormně vysokému počtu subjektu údajů a kdy není v silách správce všem oznámení učinit individuálně. Závěrem nutno podotknout, že Nařízení přímo pamatuje na situaci, kdy správce osobních údajů subjektu údajů porušení neoznámí, neboť dané porušení

[146] MORÁVEK, J. op. cit. sub 22. 228 s.
[147] Srov čl. 34 odst. 2 Nařízení.
[148] Ibid.
[149] Taková situace podle čl. 34 odst. 3 Nařízení nastane například když správce zavedl náležitá technická a organizační ochranná opatření, která byla u dotčených údajů aplikována (například způsobení nečitelnosti osobních údajů), nebo správce přijal opatření, které eliminuje jakékoli riziko do budoucna, nebo by to vyžadovalo nepřiměřené úsilí.

například nevyhodnotí jako takové, které by mohlo vést k vysokému riziku pro práva a svobody subjektů údajů. V takovém případě může dozorový orgán rozhodnout, že se o zmíněnou situaci jedná, a povinnost porušení oznámit správci udělit, případně může rozhodnout, že je naplněna jedna z výjimek dle čl. 34 odst. 3 Nařízení a správce tuto povinnost nemá.

V tomto kontextu je neméně důležité si klást otázku, jak vlastně má správce osobních údajů (který rovněž bude často právním laikem) správně posoudit, zda daný případ porušení k vysokému riziku povede, či nikoli. Pracovní skupina WP 29 v této souvislosti uvádí základní kritéria, na která se musí každý správce při tomto uvážení zaměřit a kterými jsou typ porušení, povaha, citlivost a objem osobních údajů, snadnost identifikace jednotlivců na základě těchto údajů, závažnost důsledků vyplývajících z porušení pro jednotlivce, zvláštní charakteristiky těchto jednotlivců a správce, počet dotčených jednotlivců a další obecné skutečnosti.[150][151]

Závěrem k této povinnosti správců osobních údajů je důležité zmínit jeden z významných problémů Nařízení, který v podrobnostech rozvádí například Morávek.[152] Byť je myšlenka ohlašovací a oznamovací povinnosti subjektu údajů samozřejmě správná a z teleologického hlediska nelze evropskému zákonodárci její zavedení vyčítat, naráží tento právní institut na velmi důležitou právní zásadu zvanou *nemo tenetur se ipsum accusare*. Tato zásada volným překladem znamená, že nikdo nesmí být nucen k tomu, aby poskytoval aktivní součinnost k sebeobviňování, a aby tak orgánům veřejné moci poskytoval důkazní materiál svědčící v jeho vlastní neprospěch. Je otázkou, nakolik pravidla nastavená v čl. 33 a čl. 34 Nařízení tuto právní zásadu, která je součástí práva na spravedlivý proces, vlastně narušuje a teprve čas a aplikační praxe ukáží, jak k nim budou přistupovat dozorové orgány.

Nařízení samozřejmě obsahuje ještě další vymezení povinností správce a zpracovatele subjektů údajů, které nejsou o nic méně významnější než ty popsané v této kapitole. Pro účely této práce je však dosavadní výčet s deskriptivním zhodnocením dostačujícím podkladem k tomu, aby se v dalším mohla věnovat opačnému spektru Nařízení, tedy popisu práv subjektu údajů, a aby tyto mohla práce následně ve vzájemné souvislosti zhodnotit v rámci analytické části ohledně ochrany osobních údajů v pracovněprávních vztazích se zaměřením na užívání biometriky.

---

[150] Srov. vodítko pracovní skupiny WP 29 z 3. října 2017 k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení č. WP250. 17 a 18 s.
[151] Alternativně k této problematice již vydal své pokyny i Evropský sbor pro ochrano osobních údajů ze dne 14. ledna 2021 č. 01/2021.
[152] MORÁVEK, J. op. cit. sub 22. 232 s. a násl.

4. Práva subjektu údajů dle Nařízení

Jak již bylo uvedeno v předchozí kapitole, Nařízení bylo více inovační spíše v oblasti povinnosti správců a zpracovatelů než v oblasti práv subjektu údajů. Nicméně ani oblast práv subjektu údajů, která musí být ze strany správců a zpracovatelů dodržována a respektována, aby se nedopouštěli právně závadného jednání, je z hlediska Nařízení velmi významná, a pro účely této práce je nutné se jí ve větší podrobnosti věnovat.[153] Pokud se Směrnice týče, tam byla práva subjektů údajů upravena *de facto* jen jedením ustanovením, a to čl. 12, který velmi stručně normoval, jaká práva musí členské státy prostřednictvím svých transpozičních vnitrostátních norem na ochranu osobních údajů zaručit subjektům údajů.

Problematické však bylo, že Směrnice práva subjektů neupravovala více komplexně, neboť tím pádem nezajišťovala dostatečnou garanci toho, že o svých právech subjekty údajů získají od správce dostatečné informace a že tyto budou řádně dodržovány.[154] Zároveň základní nevýhodou směrnic jako právního nástroje Evropské unie vždy bude, že členským státům pouze stanoví mantinely, ve kterých se mohou pohybovat při vytváření vlastní legislativy, ale transpozice samotná je pak často provedena nedokonale, což činí problémy nejen vnitrostátně, ale i v rámci vnitřního trhu.[155]

S ohledem na vše shora uvedené proto platí, že Nařízení je významné zejména proto, že jednotně v rámci celé Evropské unie na správce a zprostředkovatele vyvíjí vysoký tlak, aby údaje zpracovávali správně a aby u toho subjekt údajů vždy řádně o všech jeho právech informovali. V této kapitole se proto bude práce věnovat podrobněji nejdříve rozboru tzv. informace o zpracování osobních údajů dle čl. 13 a 14 Nařízení, která je základním stavebním kamenem celého procesu zpracování a následně jednotlivým právům, která subjekty údajů mají.

4.1. Informace o zpracování osobních údajů

Recitál (39) Nařízení uvádí, že: *„Pro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovány. Zásada transparentnosti vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování*

[153] Práva subjektů údajů jsou v Nařízení upravena v čl. 15 až 22.
[154] Srov. dnešní čl. 13 a 14 Nařízení, které se této problematice věnují.
[155] Důvodem je, že směrnice nemají narozdíl od nařízení přímou aplikovatelnost a nestávají se automaticky součástí právního řádu jednotlivých členských států jako nařízení.

těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Tato zásada se dotýká zejména informování subjektů údajů o totožnosti správce a účelech zpracování a o dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k dotčeným fyzickým osobám a jejich práva získat potvrzení a na sdělení zpracovávaných osobních údajů, které se jich týkají. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva." Celá právní úprava ochrany osobních údajů od přijetí Nařízení tak stojí na zásadě transparentnosti, kterou je povinen správce osobních údajů dodržovat ve vztahu ke všem subjektům, jejichž údaje zpracovává.[156]

Tato zásada je vyjádřena jednak v recitálu (39) Nařízení a jednak také v čl. 5 odst. 1 písm. a) Nařízení je blíže rozvedena v čl. 12. V tom je stanoveno, že správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v čl. 13 a 14[157] Nařízení a učinil veškerá sdělení podle čl. 15 až 22[158] a čl. 34 Nařízení. Dále toto ustanovení říká, že se informace poskytují písemně, ve vhodných případech také elektronicky, a že pokud o to subjekt údajů požádá a je prokázána jeho totožnost, může být informace poskytnuta také ústně.[159] Z uvedeného je patrné, že hlavním záměrem zákonodárce bylo při tvorbě principu transparentnosti v Nařízení co nejvíce usnadnit pozici subjektu údajů. Správce osobních údajů musí totiž vždy postupovat tak, aby byl obsah sdělovaný adresátovi jednoduše srozumitelný.[160]

Správce proto musí při plnění informační povinnosti používat jednoduchý jazyk, být co možná nejvíce stručný, subjekt údajů nezahlcovat nadbytečnými informacemi a musí primárně zajistit, aby všechny informace byly pro subjekt údajů snadno dohledatelné – jinak řečeno například odkaz na webu na informaci o zpracování osobních údajů by měl být zřetelně

[156] K podrobnějšímu výkladu k zásadě transparentnosti srov. kapitola 3 této rigorózní práce.
[157] Tyto články podrobně stanoví, jaké všechny náležitosti musí obsahovat informace o zpracování osobních údajů, jednou v případě, kdy jsou získány přímo od subjektu údajů, a jednou v případě, kdy je správce získá jiným způsobem.
[158] Tyto články Nařízení upravují jednotlivá práva subjektu údajů, jako právo na přístup, právo na opravu, právo na to být zapomenut a další.
[159] Vše upraveno v čl. 12 odst. 1 Nařízení.
[160] K tomu srov. například OTEVŘEL, R. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 14, kde je uvedeno, že: *„Taktéž je vhodné připomenout, že způsob podání informací podle komentovaného ustanovení je třeba vnímat v úzkém spojení s čl. 12, který klade například důraz na jednoduchost či srozumitelnost informací, které podle čl. 13 a 14 mají být subjektům údajů sděleny."*

viditelný a ideálně dostupný hned na úvodní stránce. Jak uvádí odborná literatura,[161] Nařízení v této souvislosti klade na správce osobních údajů v podstatě dvě protichůdné povinnosti, které je velmi obtížné splnit současně. Na straně jedné jsou totiž správci osobních údajů od účinnosti Nařízení povinni poskytovat subjektům údajů skutečně zevrubné informace, které obsahují popis všech jednotlivých práv, způsobů a možností jejich uplatnění, kontaktní informace a další sdělení nezbytná k naplnění zásady transparentnosti. Na straně druhé Nařízení správcům osobních údajů říká, že při sdělování jakýchkoli informací musí vůči subjektu údajů vystupovat tak, aby byla daná sdělení co nejsrozumitelnější a nejjednodušší.[162]

Jedním ze způsobů, jak lze dosáhnout naplnění těchto dvou protichůdných povinností ležících na bedrech správce osobních údajů, je používání tzv. vícevrstvých prohlášení či oznámení o zpracování osobních údajů/o ochraně soukromí. Pracovní skupina WP29 se k tomuto způsobu historicky opakovaně vyjadřovala, přičemž jej označila za vhodnou cestu, jak může správce osobních údajů při poskytování informaci postupovat.[163] V jednom ze svých posledních stanovisek k této problematice označení 17/CS z 29. listopadu 2017 ve znění z 11. dubna 2018 o pokynech k transparentnosti podle Nařízení se pracovní skupina WP29 věnovala užití vícevrstvých oznámení v digitálním a nedigitálním prostředí.

Pracovní skupina zde dospěla k závěru, že: *„Aby se předešlo zahlcení informacemi, WP29 zejména doporučuje použití vícevrstvých prohlášení/oznámení o ochraně soukromí, která propojí různé kategorie informací, jež subjektu údajů musejí být poskytnuty, namísto zobrazení veškerých informací v jediném oznámení na displeji. Vícevrstvá prohlášení/oznámení o ochraně soukromí mohou pomoci vyřešit napětí mezi úplností a požadavkem na srozumitelnost tím, že uživatelům umožňují přejít přímo na tu část prohlášení/oznámení, kterou si chtějí přečíst. Je třeba poznamenat, že vícevrstvá prohlášení/oznámení o ochraně soukromí nejsou jen vnořené stránky vyžadující několik kliknutí pro získání požadované informace. Vzhled a rozložení první vrstvy prohlášení/oznámení o ochraně soukromí by měly subjektu údajů nabídnout jasný přehled informací o zpracování jeho osobních údajů a o tom, kde a jak nalezne v jeho jednotlivých vrstvách podrobné informace.“*[164]

[161] MORÁVEK, J. op. cit. sub 22. 237 s.
[162] Tento rozpor je patrný při důkladném porovnání čl. 12 se zněním čl. 13 a 14 Nařízení.
[163] WP29 již dříve uznala výhody vícevrstvých oznámení ve stanovisku č. 10/2004 k jednotnějšímu poskytování informací a stanovisku č. 2/2013 k aplikacím na chytrých zařízeních.
[164] Pokyny WP29 z 29. listopadu 2017 ve znění z 11. dubna 2018 2016/679 k transparentnosti podle nařízení. 19 s.

Vrstvení informací pro subjekty údajů tak musí zaručit stejnou úroveň přehlednosti a úplnosti, jako kdyby byly všechny informace poskytované dohromady, ale umožňuje je rozdělit do samostatných podsložek, které si subjekt může detailněji nastudovat podle svého vlastního uvážení. Nejčastější v této souvislosti bývá rozvrstvení informace do tří samostatných kategorií, kdy se subjekt nejdříve dozví, co to vlastně je zpracování, proč jej správce provádí, jaký k tomu má právní titul apod. Následně po rozkliknutí druhé vrstvy zjistí, jaká má v souvislosti se zpracováním práva a jaké jsou podrobné parametry daného zpracování jako například jeho doba. A v poslední úrovni se již dozví, jak jsou jeho jednotlivá práva charakterizována a čeho všeho může jejich prostřednictvím dosáhnout.[165]

Ať již správce údajů zvolí jakoukoli metodu k naplnění zásady transparentnosti a jakýkoli způsob naplnění „vhodných opatření" ve smyslu čl. 12 odst. 1 Nařízení, vždy musí subjekt údajů informovat alespoň v takovém rozsahu, jak stanoví čl. 13 a 14 Nařízení.

4.1.1. Informace o zpracování poskytována v případě, kdy jsou osobní údaje získány přímo od subjektu údajů

Za předpokladu, že správce osobních údajů získává osobní údaje přímo od subjektu údajů, je povinen mu *a priori* sdělit vhodným způsobem tyto informace:

(i) Totožnost a kontaktní údaje správce a jeho případného zástupce – poskytují se běžné údaje jako jméno a příjmení/obchodní firma, bydliště/ sídlo, datum narození/IČO, další informace z veřejných rejstříků a kontaktní údaje jako telefonní číslo, e-mail apod.;

(ii) Má-li správce osobních údajů ustanoveného pověřence pro zpracování, musí správce informovat subjekt údajů i o totožnosti a kontaktních údajích tohoto pověřence;[166]

(iii) Účel zpracování a právní základ pro zpracování – jak je uvedeno v předchozí kapitole, správce osobních údajů je povinen zpracovávat osobní údaje jen na základě Nařízením předpokládaného právního titulu, který musí subjektu vždy sdělit (např. že zpracovává na základě souhlasu). Správce je dále povinen sdělit

[165] MORÁVEK, J. op. cit. sub 22. 237 s.
[166] Pověřenec pro ochranu osobních údajů je normován v čl. 37 a násl. Nařízení a jedná se o institut, který ve Směrnici vůbec nebyl obsažen. Tato práce se mu nicméně podrobněji věnovat nebude, neboť pro její stěžejní témata není natolik podstatným institutem.

subjektu účel zpracování, neboť jen tak může naplnit všechny zásady vztahující se k účelu vyjmenované v čl. 5 Nařízení;

(iv) Oprávněné zájmy správce nebo třetí strany v případě, že je právním titulem pro zpracování čl. 6 odst. 1 písm. f) Nařízení – Správce musí subjektu údajů sdělit, zda například zpracovává osobní údaje, aby chránil svůj majetek;[167]

(v) Případné příjemce nebo kategorie příjemců – typickým příkladem příjemců mohou být například další společnosti ze skupiny (mateřské, dceřiné, sesterské);[168]

(vi) Úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci (mimo země EU či EHP), informaci o existenci či neexistenci rozhodnutí Evropské Komise o odpovídající ochraně a odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny – vše uvedené je v Nařízení takto konkrétně specifikováno proto, že se automaticky počítá s větším rizikem porušení práv subjektu údajů v případě, kdy dochází k jejich zaslání mimo území EU, tedy mimo prostor platnosti a účinnosti Nařízení.

Čl. 13 odst. 2 Nařízení dále navíc stanoví, že vedle shora označených informací musí správce, je-li to nezbytné pro zajištění spravedlivého a transparentního zpracování, poskytnout i další informace, jež jsou vyjmenovány a podrobněji popsány níže. Platí přitom, že je právně velmi složité rozlišovat situace, ve kterých nejsou naplněny podmínky k tomu, aby se aplikoval čl. 13 odst. 2 Nařízení, pročež se odborná veřejnost kloní k tomu, že i tyto informace je lepší subjektu údajů poskytnout vždy.[169] Jedná se o:

(i) Dobu, po kterou budou údaje zpracovávány, a není-li možné ji určit, tak alespoň kritéria, podle kterých bude určena – např. zpracování údajů po dobu tří let, nebo do konce určitého procesu. Důležité je zmínit, že nestačí, pokud správce osobních údajů pouze uvede, že bude osobní údaje zpracovávat po dobu

[167] Srov. výklad JELÍNEK, T. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář*. 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020. Komentář k § 316.
[168] Srov. výklad v kapitole 2.4. této rigorózní práce.
[169] MORÁVEK, J. op. cit. sub 22. 242 s.

nezbytnou k naplnění účelu, neboť subjekt musí být vždy schopen subjektivně posoudit jasnou a zřetelnou hranici této doby;[170]

(ii) Informování o právu na přístup k osobním údajům, právo na opravu a výmaz, o právu požadovat omezení zpracování, o právu vznést námitku a o právu na přenositelnost;[171]

(iii) Právo subjektu údajů kdykoli odvolat souhlas se zpracováním osobních údajů, pokud sloužil jako právní titul k jejich zpracování ve smyslu čl. 6 odst. 1 písm. a) či čl. 9 odst. 2 písm. a) Nařízení – k naplnění této povinnosti musí správce rovněž informovat subjekt o tom, jakým způsobem lze odvolání souhlasu provést, přičemž odvolání souhlasu by mělo být stejně jednoduché jako jej poskytnout;[172]

(iv) Informování o existenci práva podat stížnost u dozorového úřadu;

(v) Skutečnost, zda je zpracování smluvním či zákonným požadavkem, zda má subjekt údajů povinnost je poskytnout a jaké jsou případné důsledky jejich neposkytnutí – typickým příkladem zákonného zpracování, kdy subjekt údajů musí informace poskytnout, neboť neposkytnutí s sebou přináší negativní důsledky, jsou pracovněprávní vztahy, ve kterých má zaměstnanec povinnost zajistit, aby o něm měl zaměstnavatel vždy aktuální údaje (například pro účely daňové a odvodové); a

(vi) Skutečnost, že dochází k automatizovanému rozhodování včetně profilování.

Odstavec 3 téhož článku pak ještě stanoví, jaké jsou další povinnosti správce osobních údajů v případě, že se mění v průběhu zpracování účel zpracování. Odstavec 4 pouze doplňuje, že informační povinnost nemá správce osobních údajů ve vztahu k těm subjektům, které již informaci mají – zde je ale nutno pamatovat na to, že má ve smyslu zásady odpovědnosti

[170] K tomu blíže také výklad v kapitole 3.5 této rigorózní práce.
[171] K tomu blíže také výklad v kapitole 4.2 a následující této rigorózní práce.
[172] Pokyny pracovní skupiny WP 29 z 29. listopadu 2017 ve znění z 11. dubna 2018 č. WP260 rev.01 k transparentnosti podle Nařízení.

důkazní břemeno k prokázání této skutečnosti správce a neposkytnutí informace z tohoto důvodu tak musí být vždy postaveno na jisto.[173]

4.1.2. Informace o zpracování poskytována v případě, kdy jsou osobní údaje získány z jiného zdroje než od subjektu údajů

Částečně odlišná situace nastává v případě, kdy je informace poskytována subjektům údajů, od kterých správce zpracovávané informace nezískal, neboť se k nim dostal z jiného zdroje. V takovém případě se oproti výše uvedenému aplikují tři rozdíly, a sice:

(i) při získání informací z jiného zdroje musí správce vždy informovat subjekt údajů o kategorii dotčených osobních údajů, tedy musí subjektu jasně popsat, jaké přesně informace z tohoto jiného zdroje získal;

(ii) je-li důvodem pro zpracování oprávněný zájem dle čl. 6 odst. 1 písm. f) Nařízení, nemusí to správce sdělovat subjektu vždy, ale jen při potřebě zajištění spravedlivého a transparentního zpracování; a

(iii) Správce musí subjektu údajů poskytnout informaci o tom, z jakého zdroje osobní údaje pocházejí, a případně informaci o tom, že pochází z veřejně přístupných zdrojů (i to musí správce sdělit jen za účelem zajištění spravedlivého a transparentního zpracování, tj. nikoli vždy).

Dále jsou na správce oproti podání informace o zpracování údajů získaných od subjektu údajů kladeny v čl. 14 Nařízení speciální povinnosti ve vztahu k tomu, do kdy musí subjektu údajů sdělit, že provádí zpracování osobních údajů získaných z jiných zdrojů. Správce tak musí učinit:

(i) Ve lhůtě přiměřené po získání údajů, nejpozději však do jednoho měsíce – pochopitelně je kladen důraz na to, aby subjekt údajů získal tuto informaci od správce co možná nejdříve;

(ii) Nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace – typickým

[173] Závěrem nutno zmínit, že vodítka pracovní skupiny WP 29 k transparentnosti podle Nařízení č. WP260 si všímají i dalších okruhů informací, které nejsou zmíněny ani v čl. 13, ale ani v čl. 14 a správce osobních údajů by je měl subjektu údajů poskytovat.

příkladem takové situace bude, když správce získá například osobní údaje o podnikatelích z veřejných rejstříků a pak je telefonicky kontaktuje za účelem nabízení určité služby či produktu; nebo

(iii) Nejpozději v okamžiku před prvním zpřístupněním těchto osobních údajů jinému příjemci, pokud má správce v plánu takový krok učinit.[174]

Správce osobních údajů přitom postupuje předně podle bodu ad (i) výše. Postupem dle ad (ii) postupuje pouze za předpokladu, že tato skutečnost nastane dříve než skutečnost označená pod bodem ad (i) a dle ad (iii) postupuje pouze, pokud skutečnost v tomto bodě předvídaná nastane dokonce dříve než ad (i) a ad (ii).[175]

Dalším významným rozdílem poskytování informací dle čl. 14 Nařízení oproti čl. 13 Nařízení je, že normuje více situací, ve kterých není správce osobních údajů povinen subjekt o jejich zpracování vůbec informovat. Kromě toho, že subjekt údajů už tuto informaci má, není správce osobních údajů povinen informaci poskytnout, vyžadovalo-li by to nepřiměřené úsilí, přičemž tento postup správce musí vždy poměřit testem proporcionality.[176] Dále není povinen správce informaci předat, pokud musí dané údaje zůstat důvěrné s ohledem na povinnost mlčenlivosti a pokud je jejich zpřístupnění výslovně a odlišně upraveno jiným právním předpisem, který má vůči Nařízení povahu *lex specialis*.

V dalším se bude práce v této kapitole věnovat jiným individuálním právům, o jejichž obsahu je správce osobních údajů rovněž povinen subjekt údajů informovat, jak zevrubně vysvětleno výše. Při celém procesu zpracování je však primární mít na paměti, že je to hlavně princip transparentnosti a úplnosti všech předaných informací, který je v oblasti ochrany osobních údajů stěžejní, a který musí všichni správci skutečně poctivě dodržovat.

Tato oblast je přitom velmi významná rovněž pro aplikační praxi, neboť informace o zpracování osobních údajů je dokument, který při tvorbě *data protection* dokumentace vzniká nejčastěji, a který také bude nejčastěji podléhat zkoumání ze strany dozorového orgánu.

---

[174] Recitál (61) Nařízení přímo uvádí: *„Informování subjektu údajů o tom, že jsou zpracovávány jeho osobní údaje, by mělo proběhnout v okamžiku jejich shromáždění od subjektu údajů, nebo pokud jsou získávány z jiného zdroje, v přiměřené lhůtě v závislosti na okolnostech případu."*

[175] MORÁVEK, J. op. cit. sub 22. 244 s.

[176] Srov. také recitál (62) Nařízení: *„Povinnost poskytnout informace však není třeba ukládat v případech, kdy subjekt údajů již uvedené informace má, nebo kdy zaznamenání či zpřístupnění osobních údajů je výslovně stanoveno právními předpisy, nebo kdy poskytnutí těchto informací subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí."*

4.2. Právo subjektu údajů na přístup k osobním údajům

Nařízení v čl. 15 normuje právo subjektu údajů na přístup údajů, které v sobě zahrnuje rovněž i právo na kopii. Toto oprávnění subjektu údajů rovněž jako právo na informace popsané shora tvoří základní kostru celého principu transparentnosti, kterým je oblast ochrany osobních údajů v dnešní době významně ovlivňována.[177] Dle zmíněného ustanovení platí, že má subjekt údajů právo získat od správce potvrzení o tom, zda dochází ke zpracování jeho osobních údajů, přičemž pokud tomu tak je, má rovněž právo získat k těmto údajům přístup.[178] Subjekt osobních údajů má v této souvislosti rovněž nárok na přístup k následujícím informacím:

(i) Účel zpracování osobních údajů a s tím pochopitelně rovněž i související právní titul, na jehož základě ke zpracování osobních údajů dochází;

(ii) Kategorie dotčených osobních údajů, tedy informace o tom, pod jakou množinu lze zařadit údaje, k jejichž zpracovávání dochází (například identifikační či kontaktní);

(iii) Příjemci nebo kategorie příjemců, kterým budou informace zpřístupněny, a to zejména příjemci ze třetích zemí, případně jedná-li se o mezinárodní organizace;

(iv) Doba, po kterou bude informace uloženy, a není-li možné ji určit konkrétně, alespoň kritéria, podle kterých bude správce tuto dobu určovat – u této kategorie informací především platí, že subjekt údajů musí vždy být schopen dobu uchování alespoň rámcově určit (tj. nepostačí, pokud správce sdělí, že osobní údaje bude zpracovávat např. po dobu nezbytně nutnou);

(v) Skutečnost, že dochází k automatizovanému rozhodování včetně;

(vi) O zdroji údajů, ze kterého správce osobní údaje získal v případě, že nejsou získány přímo od subjektu údajů (například z veřejně přístupných rejstříků); a

[177] MORÁVEK, J. op. cit. sub 22. 244 s.
[178] Pro úplnost lze zmínit, že dle předchozí právní úpravy (§ 12 ZOOÚ) poskytoval správce dle výslovného znění zákona pouze kategorie zpracovávaných osobních údajů, nikoli konkrétní zpracovávané údaje. Odborná literatura však tento výklad nezastávala, srov. POSPÍŠIL, D. in KUČEROVÁ, A., NOVÁKOVA, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2012. Komentář k § 12.

(vii) Existence práv subjektu údajů v souvislosti se zpracovávanými osobními údaji, o kterých je dále poreferováno níže jako např. právo podat stížnost u dozorového orgánu či právo na opravu.[179]

Z uvedeného výčtu jasně plyne, že právo na přístup *de facto* zrcadlí i okruh informací, které je správce povinen poskytnout v případě jeho informační povinnosti dle čl. 13 a čl. 14 Nařízení. Čl. 15 odst. 3 Nařízení pak normuje, že subjekty údajů mají kromě práva na přístup ke zmíněným informacím také právo na kopii zpracovávaných osobních údajů. Toto oprávnění má však dva významné limity.

Zaprvé, i při poskytování kopie zpracovaných osobních údajů musí vždy správce dbát toho, aby jejím poskytnutím zároveň nedocházelo k ohrožení oprávněných zájmů jiných subjektů údajů. Toto může být situace například kamerového záznamu, jehož kopii bude správce rovněž povinen poskytnout, ale bude muset předtím zajistit jeho anonymizaci, aby se tak subjekt údajů neoprávněně nedostal k osobním údajům jiných subjektů.[180]

Zadruhé, pokud by chtěl subjekt údajů tuto kopii získat opakovaně, je možné, aby správce již při druhé žádosti poskytnutí kopie přiměřeně zpoplatnil. Tento limit vložil zákonodárce do Nařízení proto, aby předcházel nedůvodným a opakovaným žádostem subjektů údajů o poskytování těchto kopií. Kromě toho je důležité zmínit, že jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, a to zejména proto, že se opakují, má správce údajů možnost odmítnout žádosti subjektu údajů.[181]

4.3. Právo subjektu údajů na opravu a výmaz osobních údajů

Podle čl. 5 písm. d) Nařízení mají správci povinnost zpracovávat osobní údaje subjektů údajů přesně. Této povinnosti odpovídá oprávnění subjektů na opravu osobních údajů za předpokladu, že správce zpracovává tyto osobní údaje nepřesně či neúplně. Při důsledném dodržování všech povinností správce tak uplatňování tohoto práva subjektu údajů nemá, resp. by nemělo mít reálný dopad do praxe, neboť i bez toho musí správce vždy zpracovávat takové údaje, které jsou přesné a úplné. Plnit tuto povinnost ze strany správce však nemusí být vždy

[179] Podle recitálu (63) Nařízení přitom platí, že: *„Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, měl by mít možnost před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká.“* a správce osobních údajů tak není povinen ve všech případech subjektu údajů bez dalšího vyhovět.
[180] K tomu srov. pokyny pracovní skupiny WP 29 ze dne 13. prosince 2016, ve znění ze dne 5. dubna 2017 č. (WP242 rev. 01) týkající se práva na přenositelnost údajů. 13 s.
[181] Srov. čl. 12 odst. 5 písm. b) Nařízení.

snadné (zejména v případě, kdy správce zpracovává osobní údaje tisíců subjektů) a uplatnění práva na opravu tak může někdy být jediný způsob, jak k opravě nepřesně či neúplně zpracovaných osobních údajů dojde. Pokud přitom správce nepřesně či neúplně zpracované osobní údaje již dříve zpřístupnil jiným příjemcům, je kromě opravy samotné rovněž vždy povinen i informovat ostatní příjemce o jejím provedení.[182]

Kromě opravy nepřesně či neúplně zpracovaných osobních údajů může subjekt údajů po správci rovněž požadovat, aby osobní údaje vymazal.[183] Jedná se o tzv. právo být zapomenut,[184] které je subjekt údajů oprávněn aktivovat a správce respektovat, nastane-li jedna z následujících okolností:

(i) Osobní údaje a jejich zpracování již nadále není potřebné – například po skončení pracovního poměru již zaměstnavatel nemusí zpracovávat všechny osobní údaje, které zpracovával v době trvání pracovního poměru;

(ii) Byl-li právním titulem pro zpracování osobních údajů souhlas subjektu údajů[185] a tento souhlas je následně odvolán, přičemž jiný právní titul pro zpracování neexistuje;

(iii) Subjekt údajů vznese námitky proti zpracování – k tomu vizte podrobněji kapitola 4.5 níže;

(iv) Osobní údaje byly zpracovány protiprávně;

(v) Osobní údaje musí být vymazány pro splnění jiné povinnosti – například když povinnost jejich výmazu stanoví rozhodnutím orgán veřejné moci; a

(vi) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 Nařízení.

Nařízení dále ve vztahu k tomuto oprávnění subjektu údajů normuje povinnost správce, aby informoval všechny ostatní správce, kteří dané osobní údaje zpracovávají, o tom, že subjekt údajů uplatnil právo na výmaz, přičemž je tak povinen učinit s ohledem na dostupnou

[182] Srov čl. 19 Nařízení, který je doplněním práva na opravu, práva na výmaz a práva na omezení zpracování.
[183] Srov. čl. 17 Nařízení.
[184] Před účinností Nařízení byla existence tohoto práva dovozena v judikatuře SDEU, konkrétně v rozhodnutí ze dne 13. května 2014, sp. zn. C-131/12, ve věci *Google Spain*,
[185] Ve smyslu čl. 6 odst. 1 písm. a) či čl. 9 odst. 2 písm. a) Nařízení.

technologii a s ohledem na přiměřené náklady. To jinými slovy také znamená, že kdyby pro správce osobních údajů byla tato povinnost spojena s nepřiměřenými náklady nebo by byla jen velmi obtížně proveditelná, nebude správce dále tížit.

V této souvislosti je nutné zmínit znění § 9 ZOZOÚ, ze kterého plyne, že pokud správce pro své příjemce vede evidenci zpracovávaných osobních údajů, do které mají příjemci přístup a která je pravidelně aktualizována, nemusí příjemce o opravě, doplnění či výmazu extra vyrozumívat, neboť tuto svou povinnost splní již samotnou aktualizací a opravou těchto osobních údajů.

V některých situacích pak správce osobních údajů nemusí žádosti subjektu údajů vyhovět, a zpracované osobní údaje tak může i nadále zpracovávat. Tyto situace taxativně vyjmenovává Nařízení v čl. 17 odst. 3 a patří mezi ně například to, když správce osobní údaje zpracovávat musí na základě povinnosti stanovené právním předpisem nebo když správce osobní údaje zpracovává za účelem určení, výkonu nebo obhajoby svých oprávněných nároků.

4.4. Právo subjektu údajů na omezení zpracování osobních údajů a na přenositelnost

Dalším z práv subjektů údajů výslovně upravených Nařízením je právo na omezení zpracování.[186] I toto právo velmi úzce souvisí hned s několika principy vyjmenovanými v čl. 5 Nařízení, a to konkrétně s principem transparentnosti, přesnosti a minimalizace údajů.[187]

Subjekt údajů může požadovat, aby správce osobních údajů omezil jejich zpracování v následujících případech:

(i) Subjekt údajů popírá přesnost zpracování osobních údajů;

(ii) Zpracování osobních údajů je protiprávní (bez právního titulu), ale subjekt údajů odmítá jejich výmaz, neboť místo něj žádá pouze o omezení;

(iii) Osobní údaje již nejsou potřebné pro původně stanovený účel zpracování, ale subjekt údajů je vyžaduje/potřebuje pro určení, výkon nebo obhajobu svých právních nároků – typickým příkladem může být situace, kdy subjekt údajů bude

[186] Srov. čl. 18 Nařízení.
[187] Srov. RÁMIŠ, V. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 18 Nařízení.

chtít uložit kamerový záznam déle, než jak správce většinou činí proto, že se jedná o důkazní materiál pro případný budoucí spor;[188] a

(iv) V případě vznesení námitky dle čl. 21 odst. 1 Nařízení, a to do doby, než bude ověřeno, zda oprávněné důvody správce nepřevažují nad oprávněnými důvody subjektu.

Pokud k omezení již zpracovaných osobních údajů došlo, může k jejich dalšímu zpracování dojít pouze se souhlasem subjektu údajů, případně pak z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv třetí osoby či z důvodu důležitého veřejného zájmu. Tak například dojde-li k omezení zpracování osobních údajů zaměstnance tak, že zaměstnavatel jako správce udržuje tyto uložené, ale jinak je nezpracovává, a zaměstnavatel zjistí, že zaměstnanec svým jednáním způsobil zaměstnavateli škodu, bude moci osobní údaje zaměstnance zpracovávat i přes existující omezení, pokud mu to pomůže v uplatnění daného nároku. I u omezení je potom důležitá opakovaně zmiňovaná transparentnost, neboť správce je povinen i v souvislosti s omezením zpracování osobních údajů kontaktovat příjemce, a má-li dojít ke zrušení omezení, musí o tom neprodleně informovat subjekt údajů.[189]

Pokud se práva na přenositelnost týče, to zaručuje subjektu údajů v určitých situacích požadovat po správci osobních údajů, aby tento správce předal ve strukturovaném, běžně používaném a strojově čitelném formátu všechny tyto osobní údaje jinému správci.

Podle čl. 20 Nařízení je subjekt údajů oprávněn tento úkon od správce požadovat tehdy, jestliže bylo původní zpracování provedeno na základě právního titulu spočívajícího v souhlasu subjektu údajů, nebo se jednalo o zpracování osobních údajů založené smlouvou. Subjekt údajů je přitom oprávněn požadovat, aby primární správce předal údaje správci sekundárnímu, je-li to technicky proveditelné, přičemž jeho žádosti nebude vyhověno, pokud by tím bylo zasaženo do práv a oprávněných zájmů třetích osob. Za technicky neproveditelné předání osobních údajů se přitom považuje situace, kdy předání není možné s ohledem na dostupné technologické možnosti správce osobních údajů nebo když by požadované úsilí k jejich předání bylo neproporcionální vzhledem k povaze předávaných údajů a rizik s jejich předáním spojených.

[188] Srov. pokyny pracovní skupiny WP29 ze dne 13. prosince 2016, ve znění ze dne 5. dubna 2017 č. (WP242 rev. 01) týkající se práva na přenositelnost údajů.
[189] Srov. čl. 19 Nařízení.

Odborná literatura k právu na přenositelnost dodatečně uvádí, že běžně používaným a strojově čitelným formátem je takový, který nevyžaduje použití zvláštní úplatné licence nebo které nevylučuje další editaci či jakoukoli jinou dispozici – z toho důvodu k naplnění práva na přenositelnost nepostačí ani předání osobních údajů ve formátu pdf.[190] Při realizaci práva na přenositelnost musí také správce zajistit, že budou předmětné osobní údaje při jejich předání dostatečně zabezpečeny.

4.5. Právo subjektu údajů vznést námitku (včetně problematiky automatizování a profilování)

Poslední část Nařízení, která normuje individuální práva subjektu údajů, je oddíl 4 týkající se práva vznést námitku a automatizovaného individuálního rozhodování.

Právo vznést námitku upravené čl. 21 Nařízení znamená, že v případě zpracování osobních údajů na základě právního titulu splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci[191] či právního titulu zpracování nezbytného pro ochranu práv a právem chráněných zájmů správce či třetí osoby[192] má subjekt údajů právo na námitku vůči konkrétnímu zpracování, a to včetně profilování založeného na těchto právních titulech (na rozdíl od práva na přenositelnost, které se na profilování nevztahuje).[193]

Po uplatnění této námitky je správce povinen přestat zpracovávat osobní údaje, pokud se mu nepodaří prokázat, že je jejich další zpracování nezbytné pro závažné důvody, které převažují nad zájmy a právy subjektu údajů, nebo že je jejich další zpracování nezbytné pro učení, výkon nebo obhajobu právních nároků.[194]

Žádná z uvedených omezení (tedy ani zpracování na základě konkrétního právního titulu, ani možnost správce osobních údajů i přes námitku dále osobní údaje zpracovávat) se neuplatní v situaci, kdy subjekt údajů námitku uplatní ve vztahu k osobním údajům, které jsou zpracovávány pro účely přímého marketingu.[195]

---

[190] MORÁVEK, J. op. cit. sub 22. 250 s.
[191] Srov. čl. 6 odst. 1 písm. e) Nařízení.
[192] Srov. čl. 6 odst. 1 písm. d) Nařízení.
[193] MORÁVEK, J. op. cit. sub 22. 250 s.
[194] Tento závěr plyne přímo z textace čl. 21 odst. 1 Nařízení, nicméně někteří autoři dovozují, že správce osobních údajů musí tyto přestat zpracovávat okamžitě, jakmile k němu námitka dojde. Srov. např NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR / Obecné nařízení o ochraně osobních údajů: praktický komentář*. Praha: Wolters Kluwer. 2017. 229 s.
[195] Srov. čl. 21 odst. 2 Nařízení.

Odst. 4 čl. 21 Nařízení jako další specifickou regulaci ve vztahu k právu vznést námitku ještě stanoví, že na toto konkrétní právo musí být subjekt údajů výslovně upozorněn a dané právo musí být uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Právo nebýt předmětem automatizovaného rozhodování včetně profilování je podrobně normováno v čl. 22 Nařízení. Profilováním se rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.[196]

Podle pracovní skupiny WP 29 má tak profilování tři základní aspekty, kterými jsou, že se musí jednat o automatizovanou formu zpracování, která je prováděna na základě osobních údajů a jejímž cílem je hodnocení osobních aspektů fyzické osoby.[197] Dle totožných pokynů pracovní skupiny WP 29 se tak profilováním rozumí shromažďování informací o určitém jednotlivci (nebo skupině jednotlivců) a hodnocení jeho charakteristik nebo vzorců chování, aby jej bylo možné zařadit do určité kategorie nebo skupiny, zejména za účelem analýzy a/nebo vytváření odhadů, například pokud jde o jejich schopnost plnit úkol, případně o jejich zájmy či pravděpodobné chování.[198]

Automatizované rozhodování na rozdíl od profilování nemá svou definici stanovenou přímo Nařízením. Podle pracovní skupiny WP 29 se za automatizované rozhodování považuje schopnost rozhodovat prostřednictvím technologických prostředků bez lidského zásahu, přičemž jeho základem mohou být jak údaje získané přímo od subjektu údajů, tak údaje odpozorované (například GPS souřadnice podle užívání aplikací), tak odvozené či vydedukované údaje, jako je profil subjektu údajů, který již byl vytvořen (například úvěrový profil).[199]

Nařízení stanoví, že subjekt údajů má právo nebýt předmětem žádného rozhodování, které je založeno na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem dotýká. Uvedené neplatí ve třech situacích, a to sice:

[196] Srov. čl. 4 bod 4) Nařízení.
[197] Srov. pokyny pracovní skupiny WP 29 ze dne 3. října 2017 s aktualizací dne 6. února 2018 č. WP251rev.01 k automatizovanému individuálnímu rozhodování a profilování pro účely Nařízení.
[198] Ibid.
[199] Ibid.

(i) Je-li takové rozhodnutí nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem osobních údajů;

(ii) Je-li takové rozhodnutí povoleno právními předpisy, které stanoví vhodná opatření zajišťující ochranu práv a oprávněných zájmů subjektu údajů; a

(iii) Je-li takové rozhodnutí založeno na výslovném souhlasu subjektu údajů.

Jinak řečeno podle čl. 22 Nařízení platí, že se v základu prosadí obecný zákaz plně automatizovaného individuálního rozhodování, včetně profilování. Existují však výjimky, ve kterých je možné automatizované individuální rozhodování, včetně profilování, připustit, a když se některá z těchto výjimek uplatní, je nutné zavést opatření, která povedou k zaručení ochrany práv subjektu údajů. Důležité rovněž je podmínku stanovenou Nařízením, že je rozhodování činěno pro *„nezbytné právní důvody či jiný akt, který by se subjektu údajů obdobně dotkl“*, vnímat široce, aby tak bylo dosaženo co nejvyšší možné ochrany subjektu údajů.[200] Ještě výraznější musí být ochrana tam, kde má na základě automatizovaného rozhodování dojít ke zpracování zvláštní kategorie osobních údajů, tedy jakýchkoli údajů citlivých, jak byly popsány shora.[201]

Automatizované rozhodování, potřeba jeho minimálního používání a práva subjektu údajů s tím spojená jsou rovněž popsána v recitálech Nařízení, kdy recitál (71) stanoví, že: *„Subjekt údajů by měl mít právo nebýt předmětem žádného rozhodnutí, a to včetně opatření, které hodnotí osobní aspekty týkající se jeho osoby, vychází výlučně z automatizovaného zpracování a které má pro něj právní účinky nebo se jej podobně významně dotýká, jako jsou automatizované zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru bez jakéhokoliv lidského zásahu. Takové zpracování zahrnuje „profilování“, jehož podstatou je jakákoliv forma automatizovaného zpracování osobních údajů hodnotící osobní aspekty vztahující se k fyzické osobě, zejména za účelem analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu, pokud má pro něj právní účinky nebo se jí podobným způsobem významně dotýká.“* Z uvedeného je tak rovněž možné dovodit, že typickým příkladem automatizovaného rozhodování bude zamítnutí žádosti subjektu údajů o poskytnutí úvěru, přičemž je-li k němu zároveň použito i profilování,

[200] MORÁVEK, J. op. cit. sub 22. 252 s.
[201] Srov čl. 22 odst. 4 Nařízení.

musí být takový postup ze strany správce co možná nejvíce omezen. Podstatné rovněž je, že základem automatizovaného rozhodování je absence jakéhokoli lidského zásahu v rámci jeho procesu, přičemž tento nelze žádným způsobem suplovat. Pracovní skupina WP 29 v této souvislosti například uvádí, že se *„Správce se nemůže vyhnout ustanovením článku 22 vykonstruováním lidského zásahu. Jestliže například někdo rutinně aplikuje na jednotlivé osoby automaticky vytvářené profily bez jakéhokoli skutečného vlivu na výsledek, jedná se stále o rozhodnutí založené výhradně na automatizovaném zpracování,"*[202]

Závěrem této kapitoly je nutné zmínit, že Nařízení kromě v této stati již popsaných institutů, právních povinností správců a zpracovatelů a práv subjektů údajů, obsahuje mnoho dalších tematických okruhů, které by svým rozsahem vydaly na samostatnou kvalifikační práci. Namátkou lze v této souvislosti například zmínit speciální úpravu obsaženou v kapitole V. Nařízení ohledně předávání osobních údajů do třetích zemí nebo mezinárodním organizacím či právní úpravu nezávislých dozorových úřadů normovanou v kapitole VI.

Cílem této rigorózní práce však není zevrubně popsat všechny jednotlivé aspekty spojené s ochranou osobních údajů upravené v Nařízení, ale propojit detailní popis těch v praxi nejvýznamnějších institutů s právní úpravou významnou v pracovněprávních vztazích, a to s důrazem na využívání moderních technologických prostředků, elektronizaci listin a využívání biometrických údajů. Jelikož uzavřením této kapitoly je první z výše stanovených úkolů v podstatě splněný, kdy práce zevrubným způsobem pomocí zejména deskriptivní metody popisuje všechny podstatné definiční pojmy, proces zpracování, povinnosti a práva dotčených subjektů a související instituty, bude v další části již pozornost věnována výlučně specifické úpravě týkající se vztahů mezi zaměstnancem a zaměstnavatelem, a to s přihlédnutím k výzvám a prostředkům moderní doby, ve které se společnost nyní nachází.

[202] Srov. pokyny pracovní skupiny WP 29 ze dne 3. října 2017 s aktualizací dne 6. února 2018 č. WP251rev.01 k automatizovanému individuálnímu rozhodování a profilování pro účely Nařízení.

5. Význam ochrany osobních údajů v pracovněprávních vztazích

Ochrana osobních údajů má v pracovněprávních vztazích své specifické a poměrně výsadní postavení. Důvodem k tomu je, že již od samého začátku pracovněprávních jednání (nábor zaměstnanců) nutně dochází ke shromažďování a zpracování osobních údajů a nelze se bez tohoto procesu obejít dokonce ani po skončení pracovněprávního vztahu (uchování osobních údajů za účelem ochrany oprávněných zájmů, z důvodů daňových etc.).

Problematiku ochrany osobních údajů v pracovněprávních vztazích proto lze mj. rozdělit podle fází těchto vztahů na jejich samostatné časové ose. Takto lze osobní údaje zaměstnance rozdělit na ty, které zaměstnavatel musí zpracovávat ještě před uzavřením pracovní smlouvy a právním vzniku pracovněprávního vztahu. Na ty, které zaměstnavatel shromažďuje a zpracovává v průběhu pracovněprávního vztahu, tedy ode dne vzniku pracovního poměru až k okamžiku jeho skončení. A na ty, které zaměstnavatel zpracovává i po skončení pracovněprávního vztahu. Že lze zpracování osobních údajů rozdělit do uvedených tří fází je možné dovodit např. i ze samotného Nařízení, kde je uvedeno, že: *„Právo členského státu nebo kolektivní smlouvy (včetně „podnikových dohod“) mohou stanovit zvláštní pravidla, která upraví zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména podmínky, za nichž lze osobní údaje v souvislosti se zaměstnáním zpracovávat na základě souhlasu zaměstnance, za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a různorodosti na pracovišti, zdraví a bezpečnosti na pracovišti, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.“*[203]

5.1. Zpracování osobních údajů v rámci výběrového řízení

Již na úvod je dobré zmínit, že většině stěžejních témat z této oblasti se věnuje stanovisko pracovní skupiny WP 29 č. 2/2017 ke zpracování osobních údajů na pracovišti ze dne 8. června 2017. Pokud se pak první z uvedených fází týče, je v této souvislosti podstatná především úprava obsažená přímo v zákoníku práce a v zákoně o zaměstnanosti. Zákoník práce totiž v ustanovení § 30 a násl. stanoví pravidla pro postup před vznikem pracovního poměru,

[203] Srov. recitál (155) Nařízení, se kterým rovněž velmi úzce souvisí čl. 88 Nařízení s názvem zpra

mezi kterými mj. je, že zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy.[204] Dané pravidlo je navíc ještě modifikováno zněním § 316 odst. 4 zákoníku práce, který stanoví demonstrativní výčet informací, které zaměstnavatel od zaměstnance vyžadovat nesmí. U některých z nich je navíc tento zákaz absolutní povahy.[205]

Již jen na základě uvedeného lze jednoznačně dovodit základní zásady zpracování osobních údajů při náborových činnostech zaměstnavatele. Při těch bude existovat sada osobních údajů, kterou bude zaměstnavatel pochopitelně shromažďovat a zpracovávat vždy, jako např. údaje kontaktní či identifikační. Kromě těch by však zaměstnavatel měl vždy velmi důkladně zvažovat, jaké další údaje bude po zaměstnancích vyžadovat a jakým způsobem (a jak dlouho) je následně bude zpracovávat. Základním východiskem viditelně je, že dané osobní údaje vždy bezpodmínečně musí souviset s pracovní pozicí, na kterou se uchazeči hlásí, a s prací, která na ní bude vykonávána. Pokud se biometrických údajů týče, jejich požadování jako tzv. zvláštních osobních údajů bude v rámci výběrových řízení většinou naprosto vyloučeno, neboť si zaměstnavatel jejich shromažďování nebude schopen nijak odůvodnit. Výjimkou v tomto ohledu může být identifikace daného uchazeče, jak bude blíže rozvedeno níže v kapitole 6. Pokud se právního titulu pro zpracování v rámci výběrových řízení týče, zaměstnavatel nebude potřebovat v případě klasického inzerování volného místa výslovný souhlas uchazečů, neboť údaje bude zpracovávat za účelem svých oprávněných zájmů a i pro účely uzavření budoucí pracovní smlouvy.[206]

Za zmínku určitě stojí také dříve hojná, ale v praxi již jednoznačně vyřešená otázka k výběrovým řízením a ochraně osobních údajů, která zní, zda zaměstnavatel může tyto uchovávat také poté, co si některého uchazeče vybere. K této problematice se ustálil názor, že zaměstnavatel je povinen takto shromážděné údaje po skončení výběrového řízení zničit,[207] pokud od daných uchazečů nezíská jejich dodatečný souhlas k jejich zpracování například za účelem budoucího oslovení na jinou pracovní pozici, která se u zaměstnavatele brzy uvolní.[208]

[204] Vizte § 30 odst. 2 zákoníku práce.
[205] Mezi tyto patří informace o sexuální orientaci, původu, členství v odborové organizaci, členství v politické stran nebo hnutí či příslušnost k církvi nebo náboženské společnosti.
[206] Tím pádem bude naplněn důvod zpracování dle čl. 6 odst. 1 písm. b) a písm. f) Nařízení.
[207] Srov. doporučení Rady Evropy z 1. dubna 2015 č. CM/Rec(2015)5.
[208] Srov např. rozhodnutí ÚOOÚ ze dne 3. října 2008, č. j. SKO-0629/07.

V závěru této části nutno podotknout, že s rozvojem moderních technologií se samostatným problémem při zpracování v rámci výběrových řízení stalo získávání údajů a oslovování potenciálních zaměstnanců na sociálních sítích. Předně je nutno podotknout, že potenciální budoucí zaměstnavatel by měl důsledně rozlišovat, na jaké sociální síti informace o svém uchazeči získává. Zatímco totiž použití například sociální platformy Linkedin, jejímž účelem je mj. také vytváření profilů za účelem náboru nových zaměstnanců a hledání práce, bude z hlediska zpracování osobních údajů pro zaměstnavatele obhajitelné, získávání informací ze soukromých profilů například na Facebooku či Instagramu již může být v rozporu s Nařízením. [209] Stejně tak pracovní skupina WP 29 byla názoru, že právě posouzení, zda má internetový profil osobní nebo obchodní povahu, je tím správným hraničním určovatelem pro posouzení, zda tyto informace může zaměstnavatel shromažďovat, či nikoli.[210]

5.2. Zpracování osobních údajů v rámci pracovního poměru

Tento časový úsek pracovního poměru zaměstnance je z hlediska zpracování osobních údajů pochopitelně tím nejpodstatnějším a také s sebou přináší nejvíce povinností na straně zaměstnavatele coby správce (zpracovatele) osobních údajů.

Zpracování osobních údajů po dobu trvání pracovního poměru úzce souvisí s úpravou obsaženou v § 312 zákoníku práce, podle kterého je zaměstnavatel oprávněn vést osobní spis zaměstnance, přičemž tento osobní spis smí obsahovat pouze písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu ve smyslu § 3 zákoníku práce. Informace a písemnosti, jež zpravidla bude osobní spis zaměstnance obsahovat, lze shromažďovat a zpracovávat opět jen v případě splnění všech zákonných povinností dle Nařízení. Pokud se právního důvodu zpracování týče, bude zaměstnavatel informace v osobním spise zpracovávat buďto za účelem splnění zákonné povinnosti (především v oblasti daňové a sociálněprávní),[211] za účelem splnění smlouvy, která byla mezi zaměstnancem a zaměstnavatelem uzavřena (například informace plynoucí z kvalifikační dohody, aby zaměstnavatel mohl řádně hradit zaměstnanci náklady související se zvyšováním kvalifikace),[212] anebo pro účely oprávněných

[209] JAROSLAV, D. *Jak by měl zaměstnavatel naložit s osobními údaji neúspěšných, ale přesto potenciálně zajímavých uchazečů o zaměstnání*. [dostupné online na pravniprostor.cz]. Právní prostor. 2019.
[210] Stanovisko pracovní skupiny WP 29 ze dne 8. června 2017 č. 2/2017 ke zpracování osobních údajů na pracovišti,. 9 s.
[211] Srov. čl. 6 odst. 1 písm. c) Nařízení.
[212] Srov. čl. 6 odst. 1 písm. b) Nařízení.

zájmů zaměstnavatele (například informace o dosaženém vzdělání, informace důležité pro bezpečnost a ochranu zdraví při práci apod.).[213][214]

Z vyjmenovaných důvodu pro zpracování ve smyslu čl. 6, resp. čl. 9 Nařízení, které mj. shodně identifikuje i odborná literatura,[215] je možné také vysledovat, co se bude rozumět písemnostmi, které jsou nezbytné pro výkon práce. Z komentářové literatury k § 312 v této souvislosti plyne, že: *„Obsahem osobního spisu nejčastěji bývají dokumenty týkající se kvalifikace zaměstnance na danou pozici (doklady o vzdělání, praxi a zkušenostech zaměstnance), dále pracovní smlouva, resp. dohoda o provedení práce či pracovní činnosti, jejich dodatky, změny či ukončení, další smlouvy uzavřené se zaměstnancem (například kvalifikační dohoda, dohoda o odpovědnosti za ztrátu svěřeného předmětu aj.), dokumenty týkající se hodnocení práce zaměstnance, případné výtky, dokumenty týkající se pracovní doby, dovolené, pracovních cest zaměstnance a jejich vyúčtování, čerpání pracovního volna, jiných překážek v práci, doklady o zdravotní způsobilosti zaměstnance, doklady o absolvovaných školeních (například BOZP), nejrůznější předávací protokoly či potvrzení apod.“*[216]

Dále může být v této rovině nápomocný také Úřad pro ochranu osobních údajů, který vydal na svých internetových stránkách seznam údajů, které může zaměstnavatel zpracovávat o svých zaměstnancích.[217] Mezi tyto patří například údaje zpracovávané za účelem správného výpočtu mzdy (vzdělání a předchozí praxe), za účelem správného výpočtu měsíčních záloh na daně, za účelem placení zdravotního pojištění, za účelem hlášení zaměstnávání cizinců atd. Všechny uvedené údaje a písemnosti mohou být v osobním spise vedené v listinné podobě, ale stejně tak je možné vést osobní spis elektronicky. Na tento způsob bude přitom ze strany zaměstnavatelů kladen stále větší důraz, neboť je to s ohledem na vývoj moderních technologií stále dostupnější a zároveň pro každého zaměstnavatele pochopitelně administrativně méně náročnější. V této souvislosti však vyvstává jeden problém související se zpracováním biometrických údajů, kterými je v tomto případě tzv. biometrický podpis. Tomu se však bude práce podrobněji věnovat v následující kapitole.

[213] Srov. čl. 6 odst. 1 písm. f) Nařízení.
[214] Srov. např. JANŠOVÁ, M. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář*. 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020. Komentář k § 312.
[215] MORÁVEK, J. op. cit. sub 22. 343 s.
[216] JANŠOVÁ, M. op. cit. sub 130.
[217] *Zaměstnavatel jako správce osobních údajů*. [dostupné online na uoou.cz]. Úřad pro ochranu osobních údajů. 2013.

Z uvedeného plyne, že penzum dokumentů, informací a údajů, které může (nebo v některých případech dokonce musí) zaměstnavatel o zaměstnanci zpracovávat, je skutečně velmi široké. V tomto kontextu je proto důležité se zabývat také otázkou, co vlastně zaměstnavatel v osobním spise o zaměstnanci evidovat nesmí. Základním určovatelem pro tuto kategorii je opakovaně zmiňovaný § 316 zákoníku práce[218], který demonstrativně vyjmenovává skupiny údajů, které zaměstnavatel v rámci pracovněprávního vztahu vyžadovat nesmí. Podle komentovaného ustanovení přitom platí, že některé informace nesmí zaměstnavatel zpracovávat nikdy (údaje o sexuální orientaci či o původu) a některé zpracovávat může, jestliže je pro to dán věcný důvod spočívající v povaze vykonávané práce (údaje o trestní bezúhonnosti).

Vzhledem k tomu, že zaměstnavatel může zpracovávat informace vztahující se pouze k vykonávané práci a musí zároveň dodržovat všechny povinnosti normované čl. 5 Nařízení, je také důležité skutečně zkoumat obsah každé doložené listiny ze strany zaměstnance, neboť může obsahovat informace, které zaměstnavatel zpracovávat může, ale zároveň i informace, které zpracovávat nesmí, protože s výkonem práce nesouvisí.[219] Stejně tak je potřeba pamatovat na to, že pokud navazuje osobní spis na údaje shromážděné a zpracované již v průběhu výběrového řízení, musí zaměstnavatel u všech těchto poměřit, zda i po konci výběrového řízení a po vzniku pracovního poměru nejsou některé údaje, které původně zpracovával, již nadbytečné, neboť se nevztahují k vykonávané práci.

Kromě zpracování osobních údajů, které jsou následně součástí osobního spisu, však zaměstnavatel nutně musí v průběhu pracovního poměru zpracovávat i osobní údaje jiné, které vznikají při samotném výkonu práce zaměstnancem. Zaměstnavatel je na straně jedné povinen řádně vést mnoho různých evidencí, kterými při případné kontrole ze strany inspektorátu práce dokládá, že je na jeho pracovišti řádně dodržován zákoník práce a související pracovněprávní předpisy. Namátkou z této podoblasti lze zmínit třeba evidenci pracovní docházky, evidenci čerpaných dovolených, evidenci související s pracovními úrazy (kniha úrazů a související oznámení), evidenci související s bezpečností a ochranou zdraví při práci (např. přehled provedených školení a účasti zaměstnanců na nich), případně evidenci související s využíváním pracovních prostředků, jako jsou například pracovní počítače, automobily, telefony apod. Na straně druhé zaměstnavatel ještě rozšiřuje oblast osobních údajů, které jsou z jeho strany

[218] Srov. JANŠOVÁ, M. op. cit. sub 214.
[219] Ibid.

zpracovávány na základě svého vlastního uvážení, a to například za účelem ochrany svých majetkových zájmů. V této rovině je velmi časté, že zaměstnavatel například používá v rámci pracoviště kamerové systémy, má kontrolu nad pracovními e-maily svých zaměstnanců, používá GPS lokátory při poskytnutí služebního automobilu apod.[220]

I při zpracování těchto osobních údajů je přitom v českém právním prostředí důležitý především § 316 zákoníku práce. Ten normuje, že zaměstnavatel je přiměřeným způsobem oprávněn kontrolovat, zda jeho zaměstnanci neužívají pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele, a to včetně jeho výpočetní techniky a telekomunikačních zařízení (internet, mobilní telefon). Stejné zákonné ustanovení dále říká, že zaměstnavatel nesmí bez závažného důvodu narušovat soukromí zaměstnanců na pracovišti tím, že by své zaměstnance podroboval skryté či otevřené kontrole spočívající ve sledování, odposlechu, záznamu telefonických hovorů či kontrole elektronické pošty. Pokud je však závažný důvod k takovým krokům dán, zaměstnavatel musí zaměstnance přímo informovat o rozsahu dané kontroly a také o způsobech jejího provádění.[221]

Ať už způsob kontroly probíhá jakkoli, je vždy důležité důkladně posoudit, zda je zde opravdu dán závažný důvod k tomu, aby zaměstnavatel mohl popsaným způsobem skutečně postupovat a užít jej v praxi. V některých případech bude kontrolu ospravedlňovat již jen samotná rizikovost vykonávané práce (např. provoz jaderné elektrárny) či stupeň důvěrnosti informací, se kterými zaměstnanci pracují (např. zaměstnanci věznice), ale v obecných a ničím specifických provozech bude uvedený postup jen málokdy plně ospravedlnitelný, neboť například ochrana majetkových hodnot sama o sobě většinou stačit nebude. Stejně tak bude muset zaměstnavatel coby správce osobních údajů ve smyslu Nařízení vždy splnit všechny povinnosti, které pro něj ze zpracování těchto osobních údajů vyplývají, tj. bude muset stanovit účel zpracování, bude muset dodržet všechny povinnosti dle čl. 5 Nařízení, bude muset své zaměstnance řádně o zpracování informovat i se všemi jejich právy ze zpracování vyplývajícími apod. To je přitom velmi podstatné, neboť většina existující judikatury Nejvyššího soudu a rozhodovací praxe ÚOOÚ k uvedeným způsobům zpracování bude ještě z doby před existencí Nařízení a ne všechny závěry tak musí být v dnešní době ještě stále aplikovatelné. Mimo to navíc stále vyvstávají nové otázky s touto problematikou související, kdy jednou

[220] Ke zpracování těchto údajů v podrobnostech srov. například stanovisko pracovní skupiny WP 29 ze dne 8. června 2017 č. 2/2017 ke zpracování osobních údajů na pracovišti.
[221] JELÍNĚK, T. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář*. 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020. Komentář k § 316.

z těch nejaktuálnějších je například kontrola zaměstnanců, kteří pracují z domova, případně odkudkoli mimo pracoviště zaměstnavatele.

Pro účely této práce je však podstatné, že v této druhé kategorii (tedy při zpracování údajů mimo písemnosti a informace ukládané do osobního spisu zaměstnance) budou zaměstnavatelé v dnešní době často používat systémy, které automaticky pracují také s biometrikou zaměstnanců daného zaměstnavatele. Je totiž již poměrně běžné, že zaměstnavatelé používají evidenční systémy postavené na identifikátorech, jakými jsou například otisk prstu či hlas, bezpečnostní systémy vycházející ze skenu obličeje či například skenu sítnice, nebo například vedení školení a rozvoje zaměstnanců pomocí jejich biometrických identifikátorů.[222] Z výše řečeného plyne, že biometrické údaje jsou v dnešní době již poměrně často využívány, a dá se očekávat, že v budoucnu podíl takto zpracovávaných údajů ještě poroste. Již jen z toho důvodu je zpracování osobních údajů především po dobu trvání pracovního poměru to, čemu se bude následující kapitola této práce věnovat nejvíc.

5.3. Zpracování osobních údajů po skončení pracovního poměru

Ani po skončení pracovního poměru však není problematika zpracování osobních údajů zaměstnance zcela vyčerpána. Již na úvod této pasáže je důležité zdůraznit, že v tomto období již zaměstnavatel zpravidla nebude o zaměstnanci zpracovávat ani shromažďovat žádné nové údaje, což mj. znamená, že ani oblast biometriky nebude v tomto čase již relevantní. Pouze pro úplnost zpracování problematiky ochrany osobních údajů v pracovněprávních vztazích je však nutno uvést, že se skončením pracovního poměru povinnosti zaměstnavatele na úseku ochrany osobních údajů rozhodně nekončí a zaměstnavatel může osobní údaje i nadále zpracovávat, i když pouze v omezeném rozsahu.[223]

Odborná literatura dělí informace, které zaměstnavatel může (musí) zpracovávat i po skončení pracovního poměru, na dvě, resp. tři kategorie, jejichž právním důvodem je buďto splnění právní povinnosti,[224] nebo oprávněné zájmy zaměstnavatele a hájení jeho práv.[225][226]

[222] K tomu srov. například kauza Metrostavu, ve které ÚOOÚ zkoumal oprávnění použití FaceID technologie k evidenci pracovní doby a ke které se práce ve větší podrobnosti vyjádří níže.
[223] KUBÍČKOVÁ, A., PATÁKOVÁ, V. *Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z*. [dostupné online na praceamzda.cz]. Práce a mzda. 2017.
[224] Srov. čl. 6 odst. 1 písm. c) Nařízení.
[225] Srov. čl. 6 odst. 1 písm. f) Nařízení.
[226] CHLÁDKOVÁ, A. *Osobní údaje v pracovněprávních vztazích – Změní se něco podle GDPR*. [dostupné online na praceamzda.cz]. Práce a mzda. 2018.

Jednu kategorii lze souhrnně označit jako penzum těch osobních údajů zaměstnanců, které zaměstnavatel i po skončení pracovního poměru zpracovává, neboť je mu tato povinnost uložena právním předpisem. Mezi ty lze zařadit např.:

(i) Dokumenty vyplývající ze zákona č. 187/2006 Sb., o nemocenském pojištění, který v § 95 stanoví, jaké informace, resp. záznamy o jakých skutečnostech musí zaměstnavatel uchovávat až po dobu deseti kalendářních roků následujících po roce, kterého se týkají, jak stanoví § 96 téhož zákona; nebo

(ii) Dokumenty a údaje stanovené zákonem č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, který např. v § 35a odst. 4 písm. a) normuje, že zaměstnavatel musí uchovávat stejnopisy evidenčních listů po dobu tří kalendářních let po roce, kterého se tyto evidenční listy týkají (tedy i po skončení zaměstnání), nebo dále v § 35a odst. 4 písm. c) normuje, že zaměstnavatel musí uchovávat záznamy o skutečnostech týkajících se účelu důchodového pojištění, a to dokonce až po dobu deseti kalendářních roků.

Do druhé, resp. třetí kategorie, spadají takové informace, které zaměstnavatel i po skončení pracovního poměru zpracovává za účelem ochrany svých vlastních práv a zájmů. Typickým příkladem takto zpracovávaných údajů mohou být všechny informace, které se například vztahují k práci vykonávané daným zaměstnancem v případě, že byl s tímto okamžitě zrušen pracovní poměr ve smyslu § 55 odst. 1 písm. b) zákoníku práce a následně je tímto zaměstnancem iniciován spor o určení neplatnosti rozvázání pracovního poměru tímto způsobem. Za takové situace je pochopitelné, že zaměstnavatel bude i nadále zpracovávat a uchovávat informace, které by byl býval normálně zlikvidoval, ale které mohou usnadnit jeho pozici při snaze unést ve sporu důkazní břemeno. U tohoto typu údajů musí však zaměstnavatel vždy řádně zvážit, po jak dlouhou dobu je může skutečně zpracovávat, přičemž nejčastěji se vychází z toho, že tak může činit po dobu prekluzivních a promlčecích lhůt k uplatnění různých práv ze strany jeho bývalých zaměstnanců.

Vše shora uvedené v této kapitole bude v kapitole následující poměřeno optikou již několikrát zmíněné biometriky. Jak je totiž na řádcích výše naznačeno, problematika ochrany osobních údajů v pracovněprávních vztazích už nesouvisí pouze s kontrolou pracovních e-mailů, využíváním kamerových systémů a GPS ve služebních autech, ale stává se se stále dostupnější technologií mnohem větší výzvou pro všechny zaměstnavatele, kteří jsou v pozici

správce (zpracovatele) osobních údajů. Biometrické údaje jsou totiž v pracovněprávních vztazích zatím relativně neprozkoumanými vodami. Poslední kapitola této práce se tak bude komplexněji dané problematice věnovat.

6. Zpracování biometrických údajů v rámci pracovněprávních vztahů

Předně je nutno zmínit, že biometrický údaj není ničím, co by se jak ve světě práva, tak mimo něj řešilo jako zbrusu nová problematika, která prozatím není blíže popsána. Tak například v oblasti ochrany osobních údajů se otázkou biometrických údajů zabývala pracovní skupina WP 29 již v roce 2003, ve kterém demonstrativně stanovila, co se může biometrickým údajem rozumět.[227] Stejně tak se biometrickým údajům okrajově věnoval rovněž ZOOÚ, jenž normoval, že citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.[228] Ani ÚOOÚ nenechal biometrické údaje stranou a věnoval se jim podrobněji v jednom ze svých stanovisek s názvem Biometrická identifikace nebo autentizace zaměstnanců.[229] V tomto stanovisku sice ÚOOÚ nepřináší žádnou ucelenou definici biometrických údajů, ale zaměřuje se podrobněji na jejich použití v pracovněprávních vztazích, například pak při jejich využívání pro přístupové a docházkové systémy. Důležité přitom je, že již v této době (tedy před přijetím Nařízení, které je ke zvláštní kategorii osobních údajů mnohem přísnější) ÚOOÚ dovozoval, že: *„Je třeba zdůraznit, že zejména biometriku založenou na zpracování citlivých údajů v centrální databázi lze v pracovněprávních vztazích využívat jen ve výjimečných situacích.“*[230]

Pokud se více aktuální a stále používané definice týče, platí podle skupiny WP 29, jak již uvedeno shora v této práci, že: *„K typickým příkladům biometrických údajů patří otisky prstů, struktura sítnice, struktura obličeje či hlas, ale také geometrie ruky, struktura žil, nebo dokonce některé hluboce zakořeněné dovednosti či jiné behaviorální rysy (například vlastnoruční podpis, úhozy na klávesnici, charakteristický způsob chůze nebo řeči atd.).“*[231] Samotné Nařízení pak v čl. 4 bodě 14 uvádí, že biometrickými údaji jsou: *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.“*, přičemž jsou dle jeho znění jednoznačně zařazeny do kategorie tzv. zvláštních osobních údajů.[232] Kromě přiřazení biometrických údajů ke zvláštní kategorii osobních údajů a stanovení určitých podmínek na

[227] Srov. stanovisko pracovní skupiny WP 29 z 1. srpna 2003 č. WP 80 o biometrice.
[228] Srov § 4 písm. b) ZOOÚ.
[229] Stanovisko Úřadu pro ochranu osobních údajů z května 2009 č. 3/2009.
[230] Ibid. 4 s.
[231] Stanovisko pracovní skupiny WP 29 ze dne 20. července 2007, č. 4/2007 WP 136.
[232] Srov. čl. 9 odst. 1 Nařízení.

tyto údaje společně například s údaji genetickými či údaji o zdravotním stavu,[233] se pak Nařízení pouze k biometrickým údajům vyjadřuje v tom smyslu, že to za splnění určitých podmínek mohou být i fotografie.[234]

Na tomto místě je rovněž důležité zmínit, že úprava definice biometrických údajů, resp. jejich striktní zařazení do zvláštní kategorie osobních údajů, s sebou přineslo jeden zásadní negativní důsledek. Před přijetím Nařízení totiž přistupoval ÚOOÚ k používání biometrických údajů v praxi poměrně rozumným způsobem, kdy striktně rozlišoval, za jakým účelem je biometrický údaj použit, a podle toho také posuzoval, zda takové zpracování spadá do roviny zpracování citlivých údajů, či nikoli.[235] S přijetím Nařízení se však ÚOOÚ vyjádřil v tom smyslu, že biometrické údaje a jejich zpracování bude nově nutné chápat tak, že správce osobních údajů vždy bude zpracovávat jednu ze zvláštních kategorií osobních údajů, a bude se na něj tak vztahovat bez dalšího čl. 9 Nařízení.[236] Takový posun je přitom pro aplikační praxi špatnou zprávou, neboť zatímco používání biometrických technologií je s ohledem na modernizaci veřejného i soukromého sektoru na vzestupu, právní úprava se v tomto ohledu stává naopak striktnější. To je přitom bohužel typickým příkladem legislativy, která absolutně neodpovídá poměrům každodenního života recipientů dané normy.

Pokud se pak konkrétní definice pojmu biometrický údaj obsažené v Nařízení týče, z té plyne, že má v dnešní době čtyři hlavní definiční znaky, kterými jsou, (i) že plyne z konkrétního technického zpracování, (ii) představuje fyzické nebo fyziologické znaky nebo znaky chování, (iii) umožňuje jedinečnou identifikaci a (iv) jedná se o osobní údaj. Pojmu osobní údaj se tato práce zevrubně věnovala již v kapitole druhé. Pokud se konkrétního technického zpracování týče, tím se jednoduše rozumí, že podle Nařízení nebude biometrickým údajem takový, který sice bude schopen naprosto jednoznačně identifikovat určitou osobu (například fotografie), ale který nebude žádným způsobem technicky zpracován, neboť v takovém případě tento údaj postrádá tzv. odvozené informace, pomocí kterých dochází v rámci jejich poměření k identifikaci dané osoby. Těmito odvozenými informacemi jsou totiž až určité specifické rysy obličeje jako vzdálenosti určitých bodů, nerovnosti a další specifické vlastnosti, které je

[233] Srov. např. recitál (53) či (91) Nařízení.
[234] Srov. recitál (51) Nařízení podle kterého se fotografie považují za biometrický údaj pouze v případě, kdy jsou zpracování zvláštními technologickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci osoby.
[235] KORBEL, F., KOVÁČ, D., NEŠPŮREK, R., OTEVŘEL, R. *Dynamický biometrický podpis nově vždy jako zvláštní kategorie osobních údajů*. Právní prostor [dostupné online na pravniprostor.cz]. Právní prostor. 10. června 2019.
[236] Srov. Změna hodnocení úrovně právní ochrany biometrických údajů ÚOOÚ ze dne 8. června 2017 dostupná online zde: https://www.uoou.cz/zmena-v-hodnoceniurovne-pravni-ochrany-biometrickych-udaju/d-23850.

schopen označit scan obličeje, a který na jejich základě například při kamerovém snímání je schopen danou osobu identifikovat a přiřadit k ní jméno, příjmení a další informace na základě fotografie registrovaného občanského průkazu či pasu.[237]

Definiční znak fyzických nebo fyziologických znaků nebo znaků chování znamená, že se v případě biometrického údaje vždy jedná o změřitelnou fyzickou či fyziologickou vlastnost živého organismu, která je dostatečně specifická a dostatečně jedinečná a stabilní na to, aby mohla sloužit jako identifikátor takového živého organismu.[238] Podle jiné definice zase tento znak biometrického údaje vychází z tzv. biometrického vzorku, kterým se rozumí anatomicko-fyziologický nebo behaviorální charakteristika dotčeného živého organismu, která se projevuje do vnějšího světa.[239] Z právního hlediska není příliš důležité rozlišovat znaky fyzické a fyziologické. Obecně však platí, že fyzické znaky jsou znaky stabilní, jako například otisk prstu či rozpoznání obličeje, a fyziologické údaje jsou znaky procesů fungování lidského těla, které jsou ovlivnitelné a různé (frekvence dýchání). Vedle těchto dále existují ještě znaky behaviorální, mezi které patří např. styl chůze nebo techniky používané jedincem při jeho vlastnoručním podpisu.[240] V této souvislosti je opakovaně důležité zmínit, že shora popsané znaky, vzorky, prvky chování a další parametry nejsou samy o sobě biometrickými údaji, neboť jsou pouze zdroji, ze kterých jsou následně biometrické údaje čerpány a shromažďovány.[241]

Posledním definičním znakem biometrických údajů uvedeným v Nařízení je tzv. jedinečná identifikovatelnost, tj. kvalita biometrického údaje, jenž umožňuje či potvrzuje správci na jeho základě naprosto konkrétní a nezpochybnitelnou identifikaci určité fyzické osoby. S tímto znakem velmi úzce souvisí dělení biometrických vzorků, prvků či rysů, které je v této práci popsáno již v kapitole 2, kdy tyto lze obecně dělit na silné biometrické rysy (například otisk prstu), slabé biometrické rysy (styl chůze) a měkké nebo jemné biometrické rysy (pouze pomocné identifikátory doprovázející zbylé dvě kategorie, jako např. věk či pohlaví).[242]

---

[237] MATEJKA, J.,, KRAUSOVÁ, A., GÜTTLER, V. *Biometrické údaje a jejich právní režim* in *Revue pro právo a technologie*. Vydání č. 17/2018. 2018. 94 s.
[238] MORDINI, E., TZOVARAS, D., (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer Netherlands. 2012.
[239] RAK, R., MATYÁŠ, V., ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, a.s. 2008. 120 s.
[240] Srov. stanovisko pracovní skupiny WP 29 z 1. srpna 2003 č. WP 80 o biometrice. 3 s.
[241] Srov. stanovisko pracovní skupiny WP 29 z 20. června 2007 č. WP 136 o konceptu osobních údajů. 9 s.
[242] MORÁVEK, J. op. cit. sub 22. 129 s. a MATEJKA, J.,, KRAUSOVÁ, A., GÜTTLER, V. op. cit. sub 237. 96 s.

Důvodem k tomu je, že na základě různých biometrických rysů lze různě složitě extrahovat biometrické údaje, které pak vedou ke schopnosti s úplnou jistotou identifikovat určitou osobu. Proces identifikace totiž probíhá tak, že dochází k porovnání jednoho biometrického vzorku s dříve uloženou šablonou, která existuje v určité databázi, a jedná se tak o porovnání jednoho s mnoha, kdy od toho, jak je daný biometrický vzorek silný, se odvíjí složitost tohoto procesu.[243] Závěrem k tomu nutno zmínit, že pro účel identifikace pro biometrické údaje vždy platí, že musí být nějakým způsobem měřitelné a jedinečné.[244] Jedinečností se v tomto kontextu rozumí, že konkrétní subjekt údajů, kterého na základě biometrického údaje identifikuji, musí být na jeho základě identifikovatelný od všech ostatních osob (zde je vidět, proč je důležité rozlišovat mezi silnými, slabými a měkkými rysy, neboť z každého z nich bude jedinečnost vyplývat s odlišnou mírou jistoty). Měřitelnost znamená, že daný rys představuje obecný identifikátor, který je dostatečně široce zastoupen ve společnosti lidí coby fyzických osob a který je možné nějakým způsobem změřit a zaznamenat. Kombinací zmíněných dvou prvků (jedinečnosti a měřitelnosti) pak může dojít k extrahování biometrických údajů z těchto rysů, neboť jakmile je k dispozici určitá měřitelná či zaznamenatelná hodnota, která je specifická pro každého jednoho člověka zvlášť (otisk prstu), je možné tohoto jedince identifikovat a odlišit od skupiny.

I když ze shora uvedeného plyne, že biometrický údaj není ničím novým a určité techniky zpracování biometrických údajů jsou staré i stovky let (například daktyloskopické zkoumání), jejich hojné využívání v pracovněprávních vztazích se stává praktické a využívané až s příchodem moderních technologií, které takový postup umožňují. Již jen s ohledem na tuto skutečnost je důležité se této otázce v souvislosti se zpracováním osobních údajů v pracovněprávních vztazích zevrubněji věnovat.

6.1. Právní titul zpracování biometrických údajů zaměstnavatelem

Jak je v této práci opakovaně zmíněno, biometrické údaje patří do tzv. zvláštní kategorie osobních údajů, která byla terminologií ZOOÚ označována souhrnně jako údaje citlivé. Kromě toho, že tedy ve vztahu k biometrickým údajům musí být splněny obecné povinnosti správce osobních údajů,[245] musí být také naplněn jeden ze zvláštních právních titulů pro jejich zpracování podle čl. 9 Nařízení. Uvedené platí proto, že podle tohoto čl. 9 je zpracování zvláštní

[243] MATEJKA, J., MATOCHOVÁ, S., PROKEŠ, J. *Analýza biometrických údajů v kontextu obecného nařízení pro ochranu osobních údajů*. Acta Informatica Pragensia. 2019. 100 s.
[244] Stanovisko pracovní skupiny WP 29 z 20. července 2007 č. 4/2007 WP 136.
[245] Srov. především čl. 5 a čl. 6 Nařízení.

kategorie osobních údajů, tedy i biometrických údajů obecně zakázáno. Členské státy dle odst. 4 ještě mohly ve vztahu k biometrickým údajům zavést další podmínky včetně omezení, toho však Česká republika nijak nevyužila. Vzhledem k této velmi přísné a restriktivní úpravě je zřejmé, že i zaměstnavatelé budou coby správci osobních údajů při jejich zpracování v mnohem horší pozici, než když budou zpracovávat osobní údaje běžné ve smyslu čl. 6 Nařízení. Práce se proto v této části bude věnovat několika právním titulům dle čl. 9 Nařízení, které budou v rámci pracovněprávních vztahů nejčastější.

6.1.1. Souhlas se zpracováním

Stejně jako u obecných právních titulů pro zpracování dle čl. 6 Nařízení i v případě zpracování zvláštní kategorie osobních údajů je souhlas subjektu údajů uváděn coby titul pro zpracování hned na prvním místě. Základní rozdíl ovšem je, že souhlas ke zpracování biometrických údajů musí být udělen výslovně, tj. nelze jej udělit generálně pro zpracování osobních údajů ze strany správce. To jinými slovy znamená, že souhlas zaměstnance se zpracováním biometrických údajů bude legitimním právním titulem pro jejich zpracování pouze za předpokladu, že bude přesně vědět, jaké biometrické údaje zaměstnavatel zpracovává, jak je zpracovává a za jakým účelem. Biometrické údaje z tohoto důvodu nepůjdou ani zahrnout do obecné informace o zpracování. I přes jejich speciální povahu nesmí zaměstnavatel zapomínat na to, že kromě speciálních povinností dle Nařízení musí splňovat i povinnosti základní.[246]

Tento právní titul zpracování má v rámci pracovněprávních vztahů jednu zásadní nevýhodu, ke které se shodně v podstatě v neprospěch zaměstnavatelů vyjadřovala jak dříve pracovní skupina WP 29, tak v současnosti Evropský sbor pro ochranu osobních údajů, a sice, že udělení souhlasu ze strany zaměstnance se zpracováním osobních údajů, a to ještě ke všemu jejich zvláštní kategorie, není ideální titul pro zpracování vzhledem k pracovněprávnímu principu subordinace.

Základním východiskem právního odvětví ochrany osobních údajů totiž je rovnost mezi správcem (zpracovatelem) a subjektem údajů, která však nemůže být v pracovněprávních vztazích nikdy zcela naplněna, když zaměstnanec vykonává svou práci ve vztahu podřízenosti k nadřízenému zaměstnavateli.[247] Pracovní skupina WP 29 a Evropský sbor pro ochranu

[246] Srov např. čl. 4 odst. 11 Nařízení podle kterého souhlas musí být svobodný, konkrétní, informovaný a jednoznačný.
[247] Srov. definice závislé práce obsažená v § 2 zákoníku práce.

osobních údajů k tomu například uvádí: *„Je nepravděpodobné, že by zaměstnanec byl schopen svobodně reagovat na žádost o udělení souhlasu zaměstnavatele například s aktivací monitorovacích systémů, jako je sledování kamerou na pracovišti, nebo s vyplněním hodnotících formulářů, aniž by cítil jakýkoli nátlak s udělením takového souhlasu"*[248] Že úřady odpovědné za podobný výklad vztahující se k souhlasu zaměstnance coby subjektu údajů tendují k takto striktnímu pojetí potom i ve světle samotného Nařízení dává perfektní smysl.[249] Kromě toho ale zároveň také nelze upřít jasné ratio logice, že zaměstnanec bude mít vždy obavu odmítnout jakýkoli požadavek ze strany zaměstnavatele, a to i když bude souviset s ochranou osobních údajů, neboť se bude bát různých forem jakékoli „odvety".

Kromě toho je dalším, v tomto případě spíše ryze praktickým problémem pro zaměstnavatele, že souhlas se zpracováním osobních údajů je právní titul, o který správce může nečekaně ze dne na den přijít, když původně udělený souhlas zaměstnanec coby subjekt údajů odvolá.[250] Tato okolnost by mohla být velmi problematická například v případě zaměstnavatele, který by ze začátku evidoval souhlas všech svých zaměstnanců s používáním například jejich otisku prstu za účelem evidování docházky. V návaznosti na takovou skutečnost by proto investoval nemalé finanční prostředky do technického provedení takové kontroly pracovní doby s tím, že by například úplně eliminoval postupy a prostředky, které k evidenci pracovní doby sloužily před tímto krokem, a následně by mu hned několik zaměstnanců takový souhlas odvolalo. Zaměstnavateli by v takovém případě nezbývalo nic jiného, než způsob evidence pracovní doby rozdvojit (přes biometrické údaje už jen pro ty, kteří souhlas neodvolali), případně ztratit již provedenou investici z důvodu potřeby přechodu na původní systém. Zejména z tohoto druhého důvodu právní titul zpracování dle čl. 9 odst. 2 písm. a) není pro zaměstnavatele ideální.

6.1.2. Plnění povinnosti a výkon zvláštních práv

Čl. 9 odst. 2 písm. b) Nařízení konkrétně jako právní titul pro zpracování osobních údajů normuje splnění povinnosti a výkonu zvláštních práv v oblasti pracovního práva a práva

[248] K tomu např. Pokyny k souhlasu podle Nařízení pracovní skupiny WP 29 z 28. listopad 2017 ve znění z 10. dubna 2018 č. WP259 rev.01. 7 s. a Pokyny Evropského sboru pro ochranu osobních údajů ze dne 4. května 2020 č. 05/2020 k souhlasu Podle Nařízení.

[249] Například recitál (42) a recitál (43) Nařízení uvádějí, že: *„souhlas by neměl být považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen."* a: *„S cílem zajistit, aby byl souhlas svobodný, by vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha (...)"*

[250] Srov čl. 7 odst. 3 Nařízení.

sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Evropské unie nebo členského státu nebo kolektivní dohodou (smlouvou) podle práva členského státu.

Z odborné komentářové literatury k dotčenému ustanovení Nařízení se podává, že: *„Typickými příklady, na které se toto ustanovení bude vztahovat, jsou údaje o zdravotním stavu zaměstnanců [těhotenství, pracovní omezení – viz ale také podobná výjimka dle čl. 9 odst. 2 písm. h)], údaj o členství v odborech pro účely hrazení příspěvků na jejich činnost, z Rakouska a Německa jsou známá zpracování údajů o náboženství pro účely daňových odvodů.“*[251] Z jiného odborného komentáře zase plyne, že se v tomto případě bude jednat o údaje zpracovávané zaměstnavatelem v souladu se zákonem č. 592/1992 Sb., o pojistném na všeobecném zdravotním pojištění, které zaměstnavatel musí nadále předávat, resp. které musí zpracovávat pro zdravotní pojišťovny.[252] Již jen z těchto úryvků odborné komentářové literatury plyne, že se právní titul pro zpracování osobních údajů dle uvedeného ustanovení pochopitelně nebude vztahovat na všechny případy, ve kterých vzniká zaměstnavateli vůči jeho zaměstnancům nějaká zákonná povinnost. To platí mj. proto, že zpracování zvláštní kategorie osobních údajů (tedy i údajů biometrických) by mělo být možné skutečně jen v těch nejvíce nezbytných případech.

Nicméně vedle případů zmíněných v daném komentáři pak lze i v rámci rozhodovací praxe ÚOOÚ narazit na rozhodnutí, kterým bylo dovozeno povolení ke zpracování biometrických údajů v důsledku plnění dalších povinností dle zákoníku práce, přičemž dané rozhodnutí se týkalo plnění povinnosti dle § 96 zákoníku práce a užívání FaceID.[253] Do budoucna proto nelze vyloučit, že se právní titul pro zpracování dle čl. 9 odst. 2 písm. b) Nařízení bude používat stále častěji, a to nikoli pouze u takových údajů, které již v dnešní době zmiňuje například komentářová literatura, ale i u údajů týkající se povinností běžnější povahy,

[251] OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 9 Nařízení.
[252] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer. 2017. Komentář k čl. 9 Nařízení.
[253] ÚOOÚ ve své kontrolní zprávě dostupné online zde: https://www.uoou.cz/kontrola-pouzivani-technologie-faceid-spolecnost-metrostav-a-s/ds-5677/archiv=1&p1=3938 uvedl: *„Vzhledem k využití technologie založené na rozpoznávání obličeje kontrolující konstatovali, že kontrolovaná osoba zpracovává i zvláštní kategorie údajů – biometrické údaje. Vzájemný vztah kontrolované osoby a dodavatele byl vyhodnocen jako vztah správce a zpracovatele, přičemž obsah rámcové smlouvy odpovídá požadavkům na smlouvu o zpracování osobních údajů dle čl. 28 odst. 3 nařízení (EU) 2016/679. Právní základ pro posuzované zpracování byl shledán v čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679 (plnění právní povinnosti), resp. pro biometrické údaje v čl. 9 odst. 2 písm. b) (plnění povinnosti v oblasti pracovního práva) ve spojení s čl. 6 odst. 1 písm. c) tohoto nařízení. Dále bylo vyhodnoceno plnění povinností, které kontrolované osobě vyplývají z čl. 5 odst. 1 písm. c) (minimalizace údajů) a čl. 5 odst. 1 písm. e) (omezení uložení) nařízení (EU) 2016/679 s tím, že kontrolovaná osoba tyto povinnosti neporušuje.“*

jako je právě například docházkový systém, evidence pracovních úrazů, dovolené a další. V každém jednotlivém případě však vždy zaměstnavatel bude muset brát ohled na to, že zpracovává zvláštní kategorii osobních údajů, a bude tak muset rozsáhle poměřovat, zda splňuje všechny zákonné povinnosti s tím spojené.

Pouze okrajově je na závěr této kapitoly nutné zmínit, že dle příslušného ustanovení Nařízení může správce osobních údajů (zaměstnavatel) tyto zpracovávat, pokud je mu to umožněno na základě kolektivní dohody (smlouvy)[254] uzavřené podle práva členského státu. Nutno však podotknout, že v České republice je toto poměrně těžko představitelné, neboť podle § 23 odst. 1 zákoníku práce platí, že: *„V kolektivní smlouvě je možné upravit práva zaměstnanců v pracovněprávních vztazích, jakož i práva nebo povinnosti smluvních stran této smlouvy. K ujednáním v kolektivní smlouvě, která zaměstnancům ukládají povinnosti nebo zkracují jejich práva stanovená tímto zákonem, se nepřihlíží.“*

6.1.3. Ochrana životně důležitých zájmů

Kapitola 3. této práce věnující se jednotlivým titulům pro zpracování osobních údajů dle čl. 6 Nařízení je co do otázky právního titulu dle čl. 9 odst. 2 písm. c) plně použitelná, neboť tento právní titul je jak dle čl. 6, tak dle čl. 9 Nařízení velmi obdobný a lze na oba případy vztáhnout stejné závěry. Rozhodující tak je v obou případech recitál (46) Nařízení[255] a skutečnost, že dotčený právní titul pro zpracování tvoří v jejich celkové hierarchii jakési *ultima ratio*, tj. lze na jeho základě osobní údaje zpracovávat pouze tehdy, pokud nepřipadá v úvahu žádný jiný titul. Zásadním rozdílem v úpravě obsažené v čl. 9 oproti čl. 6 Nařízení je však to, že zvláštní kategorii osobních údajů (tedy i údaje biometrické) lze na základě čl. 9 odst. 2 písm. c) zpracovávat jen tehdy, pokud není z nějakého objektivního důvodu[256] možné získat k tomu souhlas subjektu údajů.

V pracovněprávních vztazích bude tento právní titul pro zpracování biometrických údajů pravděpodobně velmi ojedinělý. Lze si však představit, že bude možné na jeho základě zpracovat osobní údaje biometrické povahy speciálně v případě závažného pracovního úrazu

[254] V rámci Nařízení neexistuje mezi pojmy „dohoda“ a „smlouva“ v kontextu kolektivního pracovního práva žádný rozdíl srov. OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. op. cit. sub. 251.

[255] *„Zpracování osobních údajů na základě životně důležitého zájmu jiné fyzické osoby by mělo v zásadě proběhnout pouze tehdy, pokud zjevně nemůže být založeno na jiném právním základě“*

[256] Srov. OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. op. cit. sub. 251, kde se uvádí, že daná překážka může být časové povahy (subjekt údajů nemůže souhlas poskytnout včas), geografické (subjekt údajů se nachází jinde a nelze použít k jeho dostižení telekomunikační prostředky) či právní (subjekt údajů byl zbaven svéprávnosti).

zaměstnance. Zaměstnavatel může při snaze odvrátit vážné zdravotní důsledky nebo např. i smrt zaměstnance[257] v daném případě zpracovat informaci týkající se jeho krve (typ, krevní anamnézu) či vztahující se k jeho DNA. Jak však plyne z odborné literatury, jakmile odpadne překážka, pro kterou nebylo možno získat souhlas přímo subjektu údajů, je správce povinen jej buďto získat, nebo přistoupit k okamžité likvidaci zpracovaných osobních údajů.[258]

Vzhledem k mizivé aplikovatelnosti komentovaného titulu pro zpracování osobních údajů v praxi pracovněprávních vztahů mu dále nebude věnována větší pozornost.

6.1.4. Neziskový subjekt zaměstnavatelem

Že je tento právní titul pro zpracování biometrických údajů relevantní i v pracovněprávních vztazích, plyne již z komentářové literatury, která pro jeho užití uvádí tři základní podmínky, a sice:

(i) Správcem osobních údajů musí být nadace nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle;

(ii) Zpracování musí být prováděno v rámci oprávněných činností takového subjektu; a

(iii) Subjekty údajů jsou součástí, členové či zaměstnanci a jiný personál důležitý pro chod takového subjektu, případně osoby, které s ním udržují pravidelné styky a jsou pro jeho chod rovněž důležitý (sponzoři).[259]

Uvedený právní titul pro zpracování normovaný v čl. 9 odst. 2 písm. d) Nařízení má ještě několik dalších zvláštností. V prvé řadě Nařízení výslovně stanoví, že údaje zpracované na jeho základě nemohou být bez souhlasu subjektu údajů zpřístupněny mimo subjekt zpracování osobních údajů. Stejně tak na základě tohoto právního titulu nemohou osobní údaje zpracovávat všechny subjekty, ale pouze ty vymezené v daném ustanovení Nařízení, přičemž základním rozlišujícím prvkem pro jejich určení je jejich neziskovost, tj. jejich primární činnost nesmí být vyvíjena za účelem dosažení určitého zisku (to je možné jen v případě činnosti

[257] Například podle stanoviska pracovní skupiny WP 29 z 9. dubna 2014 č. WP 217 platí, že „životně důležitý zájem“ se skutečně vztahuje k otázkám života a smrti subjektu údajů, nebo nejméně se jedná alespoň o takovou situaci, v jejímž důsledku by mohl být život či zdraví subjektu údajů vážně ohrožen (srov. 20 s. dotčeného stanoviska).
[258] Ibid.
[259] Srov. OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. op. cit. sub. 251.

vedlejší, kdy je daný zisk navíc nadále použit pro účely rozvoje dotčeného subjektu).[260] Konkrétnější identifikace subjektů, které budou moci na základě tohoto právního titulu zpracovávat informace, plyne také z typového výčtu údajů, o kterých čl. 9 odst. 2 písm. d) hovoří. Bude se tak zpravidla jednat o náboženské organizace, politické strany, případně také odborové organizace.

Přes vše shora uvedené platí, že byť zpracování biometrických údajů na základě tohoto právního titulu v pracovněprávních vztazích je možné a obecně pro něj jsou splněny všechny zákonné podmínky, stejně jako v případě předchozí podkapitoly, ani tento nebude hojně využívaný, pročež nebude v rovině pracovněprávní ani problematický. To především proto, že i když nadace bude například evidovat docházku svých zaměstnanců pomocí zpracování jejich otisků prstů, bude tak činit spíše na základě jejich výslovného souhlasu dle čl. 9 odst. 2 písm. a) Nařízení, případně z důvodu plnění zákonných povinností správce.

6.1.5. Ostatní právní tituly pro zpracování dle čl. 9

U všech ostatních právních titulů pro zpracování zvláštní kategorie osobních údajů (tj. i údajů biometrických) je pro jejich potenciální využití v pracovněprávních vztazích skutečně minimální prostor. Ať už se jedná o takové, jejichž užití bude pro zpracování biometrických údajů v pracovněprávních vztazích již z podstaty věci přímo vyloučeno (archivace, vědecký či historický vědecký výzkum), nebo o takové, které bude možno použít skutečně pouze výjimečně (určení, výkon a obhajoba právních nároků), žádný z daných titulů není s ohledem na zaměření této poslední kapitoly natolik relevantní, aby mu byl věnován větší prostor.

6.1.6. Významný veřejný zájem existující na základě práva

Speciální situací, která na závěr této podkapitoly stojí za zmínku, je zpracování zvláštní kategorie osobních údajů na základě přímého znění zákona. Existují totiž právní předpisy, které zpracování biometrických údajů obsahují přímo ve svém normativním textu. Příkladem takového zákona je zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon v § 24 normuje, že se pro zabezpečení ochrany utajovaných informací na jeho základě určují v rámci fyzické bezpečnosti objekty, zabezpečené oblasti a jednací oblasti. V návaznosti na to je v § 29 totožného zákona řečeno, že režimová opatření stanoví oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, oprávnění osob pro vstup

[260] NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. op. cit. sub. 252.

do zabezpečené oblasti a jednací oblasti a způsob kontroly těchto oprávnění a způsob manipulace s technickými prostředky. Jako jeden z technických prostředků potom § 30 odst. 1 písm. b) tohoto zákona stanoví elektrické zámkové zařízení a systémy pro kontrolu vstupů, což jinými slovy znamená, že na základě tohoto právního předpisu je možné zpracovávat biometrické údaje (např. otisky prstů) osob, které mají např. přístup do objektů ve smyslu takového zákona. Zpravidla se přitom bude jednat o osoby pověřené k takovému postupu, které budou například součástí ostrahy, a tím pádem se na ně daná povinnost bude vztahovat z existence jejich pracovněprávního vztahu.

Dalším obdobným příkladem je zpracování biometrických údajů na základě vyhlášky č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu, jež byla vydána k doplnění a provedení zákona č. 263/2016 Sb., atomový zákon. V atomovém zákoně jsou hned v jeho § 4 obsaženy definice základních pojmů, mezi které patří například vnitřní, životně důležitý, chráněný nebo střežený prostor (§ 4 odst. 1 písm. f), g), h) a i). V dotčené vyhlášce je pak mj. řečeno, že kdo je oprávněn vstupovat do těchto prostorů, musí být vybaven identifikační kartou umožňující automatickou kontrolu vstupu, přičemž pro vstup do některých z těchto prostorů musí být použita biometrický identifikace. Před takovým vstupem tak u osob oprávněných k těmto vstupům musí jednoznačně dojít ke zpracování jejich biometrických údajů, jejich shromažďování a následnému ukládání, přičemž stejně jako v příkladě předchozím dle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti se i za této situace bude jednat o takové osoby, které jsou k těmto vstupům oprávněny z titulu svého pracovněprávního zařazení k určitému subjektu.

Jelikož se práce již zabývala specifikací pojmu biometrický údaj a vypořádala se s problematikou, za jakých okolností vlastně zaměstnavatelé budou moci biometrické údaje svých zaměstnanců zpracovávat, přistoupí v následující kapitole k jednotlivým typům zpracování biometrických údajů v pracovněprávních vztazích a jejich problematickým aspektům.

6.2. Typy zpracování biometrických údajů v zaměstnání před vznikem pracovněprávního vztahu a v jeho průběhu

V následující části se bude tato rigorózní práce věnovat konkrétním případům, ve kterých může v rámci pracovněprávních vztahů docházet ke zpracování biometrických údajů. Je přitom nezbytné vykládat ji v kontextu jak s předchozí kapitolou, tak s ostatními částmi

kapitoly této, neboť pouze takto v souhrnu je zřetelně vidět, jak velký problém může současný přístup ke zpracování biometrických údajů v pracovněprávních vztazích do budoucna být. Účelem této kapitoly přitom není popsat všechny situace, ve kterých může zaměstnavatel biometrické údaje svých zaměstnanců zpracovávat, ale více přiblížit ty oblasti, které jsou v praxi pravděpodobně nejčastější.

6.2.1. Výběrové řízení pro nové zaměstnance

Podle zprávy americké Federální obchodní komise *Consumer Sentinel Network* z února 2021 docházelo nejen ve spotřebitelsko-právních, ale i ostatních druzích právních vztahů nejčastěji k podvodům, které souvisí s elektronickou krádeží identity/osobnosti.[261] Z toho plyne, že je v dnešní době potřeba klást stále větší důraz na ochranu v elektronickém a virtuálním světě, kde jsou podobné útoky pořád častější. To pochopitelně platí i pro zaměstnavatele, u kterých probíhá výběrové řízení na jakékoli volné pracovní místo v jejich organizační struktuře. Tovární systém zaměstnávání, kdy každý zaměstnanec chodil fyzicky každý den do práce a stejně tak se musel fyzicky ukázat i v rámci přijímacího řízení, je přitom dávnou minulostí a stále větší procento prací i v hlavním pracovním poměru se dneska odehrává pouze virtuálně a dálkově. Technicky vzato tak v dnešní době není vyloučeno, aby zaměstnavatel přijal do pracovněprávního vztahu uchazeče, kterého nikdy fyzicky neviděl a za dobu trvání pracovního poměru ho nikdy ani fyzicky neuvidí.

I v souvislosti s tím pak samozřejmě vyvstává otázka, jak se ještě před zahájením pracovního poměru dá bránit tomu, aby například konkrétní zaměstnavatel nepřijal a následně nezpřístupnil své obchodní tajemství a jiné citlivé údaje někomu, jehož jediným cílem je tyto zpronevěřit a zaměstnavateli tak uškodit. K tomu může sloužit tzv. *Identity Proofing*, což je technologie, která slouží k ověření a autentizaci identity osoby, která se přihlašuje do určité aplikace, komunikuje pouze pomocí elektronických prostředků na dálku apod.[262]

V dnešní době se již jedná o produkt, který je naprosto běžně komerčně nabízen, a to nikoli jen a pouze v rámci pracovněprávních vztahů, ale také například pro naplnění některých druhů povinností v rámci běžného obchodu, jako je například KYC.[263] *Identity Proofing* je přitom možné provést několika různými technikami. Mezi ty nejzákladnější patří i všem známá verifikace, že osoba, která například používá nějaký formulář, objednává něco na internetu či se přihlašuje k nějaké aktivitě není robot, což potvrdí například tím, že z obrazovky opíše jakýsi unikátní kód. Sofistikovanější metody zahrnují například tzv. *Face Matching* či *Liveness Check*.[264]

[261] FEDERAL TRADE COMMISION, CONSUMER SENTINEL NETWORK. *Data Book 2020*. Únor 2021. 6 s.
[262] SHAM, S. *What is Identity Proofing?* [dostupné online z okta.com]. OKTA. 2019.
[263] KYC je zkratka pro výraz *Know Your Customer*, tedy v překladu *Poznej svého zákazníka*, který je používán a se kterým musí být v souladu zejména finanční instituce při poskytování úvěrů a jiných bankovních služeb. V rámci Evropské unie tento pojem souvisí s balíčkem práv a povinností souhrnně subsumovaných pod tzv. AML předpisy, tedy předpisy sloužící na ochranu proti terorismu a praní špinavých peněz.
[264] Srov. například produkty nabízené v této oblasti od společností Verifai. či Entrust.

Face Matching spočívá v tom, že kandidát je povinen nejdříve, např. ještě před zahájením přijímacího pohovoru, nahrát do počítačového rozhraní potenciálního budoucího zaměstnavatele svůj identifikační doklad, jako například pas či občanský průkaz. Následně je kandidát ze strany osoby, která tento pohovor vede, vyzván, aby si vyfotil *selfie*, která se automaticky nahraje do systému, ve kterém je již evidován jeho identifikační doklad. Tento systém následně pomocí zpracování biometrických údajů dokáže rozpoznat, zda osoba, která se přijímacího pohovoru účastní, je skutečně ten člověk, který o sobě uvedl údaje na dříve předloženém identifikačním dokumentu.

Liveness Check je potom ještě o něco sofistikovanější systém, který může posloužit v takových případech, kdy někdo již dříve odcizil jiné osobě její občanský průkaz a má k dispozici její *selfie,* a snažil by se tak obejít systém *Face Matchingu*. V rámci této druhé aplikace je totiž člověk mj. povinen přímo v rámci přijímacího pohovoru učinit několik velmi jednoduchých úkolů s pomocí svého obličeje/hlavy, které nelze nikdy vědět dopředu. Může se jednat o otočení hlavy, vyslovení nějakého slova, o úsměv, zamračení a další. Technologie *Liveness Check* dokáže na základě těchto jednoduchých úkolů určit, s jakou pravděpodobností je veden přijímací pohovor skutečně s osobou, která se k němu původně přihlásila. V budoucnu přitom užívání podobných technologií lze očekávat stále častěji, a to se stále větším rozmachem *remote work*, více druhy práce, které umožňují vykonávat práci na dálku apod.

Je sice pravdou, že již v této rovině zaměstnavatelům v podstatě podle Nařízení chybí právní titul, na jehož základě by bylo možné tyto biometrické údaje zpracovávat, ale lze si jistě představit udělení výslovného souhlasu ze strany konkrétního uchazeče a dále také zpracování pro účely určení, výkon nebo obhajobu právních nároků, kdy s rostoucím rizikem shora zmíněného *Identity Theft* bude kladen větší důraz na to, aby měli zaměstnavatelé možnost, jak se těmto postupům bránit. To vše samozřejmě vždy za předpokladu, že bude potenciální budoucí zaměstnavatel dodržovat povinnosti dle jiných právních předpisů.[265]

6.2.2. *Paperless* spis zaměstnanců

V kapitole 5. této rigorózní práce již bylo pojednáno o tom, že v průběhu trvání pracovněprávního vztahu dochází pravidelně k vytvoření tzv. osobního spisu zaměstnance.[266] V dnešní době stále větší elektronizace a digitalizace je však žádoucí, aby i osobní spis

[265] Srov. například ustanovení § 30 zákoníku práce nebo § 12 zákona o zaměstnanosti.
[266] Srov. § 312 zákoníku práce, podle kterého smí osobní spis obsahovat pouze písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu ve smyslu § 3 zákoníku práce.

zaměstnance mohl být veden pouze v elektronické podobě a aby dokumenty podstatné v rámci pracovněprávního vztahu nemusel zaměstnavatel uchovávat nikde v listinné podobě. Takový požadavek u většiny dokumentace, která se v osobních spise normálně nachází (evidenční listy důchodového pojištění, mzdové listy, evidence docházky a dovolené, informace k DPN apod.), problematická nebude. U některých dokumentů je však zákoníkem práce stanoveno, že musí být vyhotoveny, resp. uzavřeny písemně, a otázkou tak je, zda bude tato podmínka splněna, když i takové listiny bude mít zaměstnavatel pouze v elektronické podobě.

Zákoník práce však žádné speciální požadavky na písemnou formu nestanoví a užije se tak obecná úprava vyplývající z občanského zákoníku obsažená v § 559 a následující. Z toho plyne, že i pracovněprávní dokument (např. pracovní smlouva) vyžadující písemnou formu bude tuto náležitost splňovat, když bude zachycen v elektronickém formátu (např. PDF)[267] a bude obsahovat elektronické podpisy.[268] Jako ideální způsob, jak pracovněprávní dokumentaci elektronicky podepisovat, se jeví tzv. dynamický biometrický podpis, neboť ten je pevně spojen s konkrétním dokumentem a umožňuje autentizaci podepisující osoby.[269] Dynamické biometrické podpisy mají dle současné účinné legislativy povahu tzv. prostého elektronického podpisu,[270] jenž je uznáván jako platný typ podpisu soukromoprávních jednání.[271] Tento podpis je přitom ve srovnání s jinými prostými podpisy (například uvedením pouhého jména a příjmení pod e-mail) specifický tím, že má mnohem vyšší potenciál autentizace osoby, která jeho prostřednictvím dokument podepsala, pročež má mnohem vyšší důkazní sílu v případě, kdy je nutné prokázat, že byl daný dokument podepsán určitou osobou, neboť zachycuje biometrickou stopu podepisující osoby (sklon pera, tlak, rychlost a další).[272]

To vše jinými slovy znamená, že při užití dynamického biometrického podpisu dochází ke zpracování biometrických údajů konkrétního zaměstnance, a opět tak v souvislosti s takovým postupem bude nutné naplnit všechny povinnosti dle Nařízení včetně stanovení právního titulu pro jejich zpracování. V této rovině rovněž není bez významu shora již jednou

[267] Srov. § 562 občanského zákoníku.
[268] Srov. § 561 občanského zákoníku.
[269] Srov. ŠKUBAL, J., VEJSADA D. *Elektronický personální spis*. Práce a Mzda. 2. ledna 2019. 2 s.
[270] Dle definice čl. 3 bodu 10 nařízení Evropského parlamentu a Rady (EU) č. 910/2014, které stanoví, že: *„elektronickým podpisem" se rozumí data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“.*
[271] Dle § 7 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
[272] K povaze dynamického biometrického podpisu blíže například SMEJKAL V. *Kryptografický a dynamický biometrický podpis podle platné právní úpravy*. Právní rozhledy. č. 10/2019. 43 s.

citované rozhodnutí ÚOOÚ, které minimálně ve finančním sektoru ve spotřebitelských vztazích označilo dynamický biometrický podpis za nevyhovující pravidlům Nařízení.[273]

Kromě naplnění povinnosti dle Nařízení existuje však v případě vedení elektronického spisu zaměstnance obsahujícího všechny dokumenty ještě jeden zásadní problém, a tím je právní úprava doručování v pracovněprávních vztazích.[274] Zákoník práce totiž stanoví, že písemnosti týkající se vzniku, změn a skončení pracovního poměru nebo dohod o pracích konaných mimo pracovní poměr, odvolání z pracovního místa vedoucího zaměstnance, důležité písemnosti týkající se odměňování a záznam o porušení režimu dočasně práce neschopného pojištěnce musí být doručeny zaměstnanci do vlastních rukou. Takovým doručením se rozumí jejich doručení na pracovišti, a není-li to možné, tak alternativně, a to buďto kdekoli bude zaměstnanec zastižen, prostřednictvím provozovatele poštovních služeb, prostřednictvím sítě nebo služby elektronických komunikací nebo prostřednictvím datové schránky.

V diskutovaném případě by bylo možné uvažovat o doručování prostřednictvím sítě nebo služby elektronických komunikací. To však lze dle zákoníku práce využívat pouze za splnění přísných zákonných požadavků, jakými jsou (i) předchozí souhlas zaměstnance, který musí být učiněn písemně, (ii) opatření písemnosti doručované prostřednictvím sítě nebo služby elektronických komunikací uznávaným elektronickým podpisem a (iii) potvrzení zaměstnance o doručení daného dokumentu, a to uznávaným elektronickým podpisem. Kromě toho také elektronické dokumenty ještě lze zasílat datovou schránkou, ale u té bude pořád nejčastějším problémem fakt, že ji málo zaměstnanců bude mít zřízenou.[275]

Tento problém bude poměrně zásadní povahy především u jednostranných právních jednání a faktických úkonů v pracovněprávních vztazích, neboť jejich účinnost je často spojena právě až s doručením takového dokumentu. Primárně je přitom vždy nutné doručit zaměstnanci dokument do vlastních rukou na pracovišti a zákoník práce nepočítá s tím, že se tak může stát například i na elektronickém nosiči dat (např. na flash-disku nebo uložením do speciálního osobního spisu zaměstnance dostupného na intranetu dané společnosti). Novela zákoníku práce účinná od 30. července 2021, resp. od 1. ledna 2021, doručování sice částečně změnila a také jej v mnoha ohledech zásadně zjednodušila, ale v této konkrétní rovině jednoznačnou odpověď nenabídla. V následujících letech je proto pořád nejisté, zda bude užívání dynamických

[273] Rozhodnutí ÚOOÚ z 21. března 2019, č. j. UOOU-10138/18-8.
[274] Srov. § 334 a násl zákoníku práce.
[275] Srov. § 335 a § 335a zákoníku práce.

biometrických podpisů a elektronické vedení osobních spisů zaměstnanců možné a zda nebude zaměstnavatelům přinášet více problémů než užitku.

6.2.3. Systémy vztahující se k přístupům a k docházce

Řízení přístupu a evidence docházky jsou v oblasti užívání biometrických technologií těmi možná nejprotežovanejšími tématy. V této práci o nich bude pojednáno souhrnně především proto, že do budoucna lze očekávat snahu zkombinovat na pracovišti jeden technologický přístupový systém, který bude nejenom zabezpečovat pracoviště určitého zaměstnavatele, ale zároveň bude evidovat, kdy jednotliví zaměstnanci do práce přichází a kdy zase odchází.

Pokud se řízení přístupu týče, označuje se tím obecně jakákoli technologie, která je používána za účelem kontroly a zabezpečení přístupu do jakéhokoli prostředí či rozhraní, a to bez ohledu na to, zda kamenného, či digitálního. Svým způsobem lze mezi řízení přístupu zařadit i vynález zamykacích dveří, kdy na konkrétní pracoviště mají přístup pomocí běžného klíče jen zaměstnanci daného zaměstnavatele. Řízení přístupu je také součástí našeho každodenního života, neboť i každé zabezpečení našich mobilních telefonů od zadávání pinů až po odemykání na základě otisku prstu je kategorií, která do řízení přístupu spadá.

Podstatné tak je si uvědomit, že když mluvíme o řízení přístupů, nebude se jednat pouze o vstup do budovy, skladu, kanceláří či laboratoří, ale také například o vzdálený přístup do počítačového rozhraní, ve kterém lze vykonávat práci pro svého zaměstnavatele. Zejména u posledního zmíněného lze i nadále díky stále přítomné pandemii čekat stále větší rozmach, neboť jen od začátku pandemie v březnu roku 2020 docházelo k rapidnímu zvyšování čísel lidí pracujících na home-office, a to až o desítky procent, což lze také dovodit z oficiálních statistik společnosti Microsoft o tom, jak se zvýšilo užívání softwarových platforem sloužících k dálkové komunikaci a práci.[276] I mimo digitální svět je však užívání přístupových systémů s větším důrazem na technologie na vzestupu, neboť například využívání biometrických

[276] Srov. například ŠTUKOVA, K.: *Česko pracuje z domova. V některých firmách až půlka zaměstnanců*. [dostupné online na idnes.cz]. IDNES. Publikováno dne 11. března 2020 či ČTK, IDNES.cz: *Třetina zaměstnanců pracuje podle průzkumu z domova, část z nich ruší rodina*. Publikováno dne 23. března 2020. [dostupné online na idnes.cz]. IDNES. K užívání některých platforem Microsoft srov. SPATARO, J.: *Remote work trend report: meetings*. [dostupné online z microsoft.com].

technologií fungujících na bázi otisku prstu, skenu sítnice či obličeje apod. vzroste podle různých předpokladů do roku 2022 až na 70 %, zatímco v roce 2018 to bylo pouze 5 %.[277]

Ve vztahu k právní stránce ochrany osobních údajů se touto problematikou okrajově zabývá také jedno ze stanovisek Evropského sboru pro ochranu osobních údajů č. 3/2019 z 29. ledna 2020, a to především v bodě 77 a násl. tohoto stanoviska.[278] Z toho plyne, že zpracování biometrických údajů v rámci přístupu řízení bude většinou založeno na výslovném souhlasu subjektu údajů, což bude rovněž platit pro oblast pracovněprávních vztahů. Problematické v tomto ohledu však je, jak bylo shora již několikrát zmíněno, že vztah mezi zaměstnavatelem a zaměstnancem je vztah nadřízenosti a podřízenosti a zaměstnanec by za žádných okolností neměl být nucen k udělení souhlasu se zpracováním svých biometrických údajů, přičemž pokud by zaměstnavatel jiný vstup na pracoviště neumožňoval, v podstatě by zaměstnance k takovému postupu skutečně donutil. Možným řešením tohoto problému je, že zaměstnanci budou mít na výběr, jakým způsobem budou u vstupu kontrolováni a jak bude řízení přístupu prováděno. Například budou mít možnost dát výslovný souhlas se zpracováním svého biometrického údaje v podobě otisku prstu, přes který se pak budou moci dostat do všech chráněných prostor na pracovišti, nebo si nechat od zaměstnavatele udělit klasickou přístupovou kartu, která je dnes naprosto běžným nástrojem řízení přístupů. Jelikož je první volba uživatelsky pro všechny zúčastněné příjemnější (a to již jen proto, že otisk prstu nelze například ztratit), lze očekávat, že se takový postup zaměstnavateli vyplatí a většina zaměstnanců svůj souhlas udělí.

Mezi příklady řízení přístupu lze zařadit technologie jako (i) rozpoznávání otisku prstu, (ii) 2D rozpoznávání obličeje, které funguje tak, že je zachycen obrázek obličeje určitého jedince, který je pomocí matematických operací poměřen s uloženým vzorem, a pokud jsou oba zdroje dat v souladu, je umožněn přístup, (iii) 3D rozpoznávání obličeje, které funguje obdobně jako 2D systém s tím rozdílem, že je kombinací více snímků vytvořen 3D model celého obličeje daného jedince včetně všech záhybů, vrásek apod., což umožňuje lepší míru identifikace a autentizace, (iv) identifikace duhovky, která funguje stejně jako 2D rozpoznávání obličeje či (v) geometrie ruky, která funguje podobně jako 3D rozpoznávání obličeje, kdy je vytvořen

[277] OMALE, G. *Gartner Predicts Increased Adoption of Mobile-Centric Biometric Authentification and Saas-Delivered IAM*. [dostupné online z Gartner.com]. Gartner. Egham, Velká Británie, 6. února 2019.
[278] Pokyny Evropského sboru pro ochranu osobních údajů z 29. ledna 2020 č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky.

snímek, který pomocí matematických operací určí délku prstů, tvar a velikost ruky a další kritéria a poměří je s uloženým vzorem.[279]

U docházkových systémů je pak situace částečně odlišná, neboť zatímco řízení přístupu je v podstatě používáno jenom za účelem ochrany zájmů zaměstnavatele, který tak činí čistě dobrovolně a bez jakékoli příčiny, evidence docházky a vedení docházkových systémů je naprosto stěžejní prvek pro zásadní povinnosti normované zákoníkem práce. V této práci již bylo zmíněno, že zaměstnavatel je povinen vést u jednotlivých zaměstnanců evidenci začátku a konce jejich odpracované směny, práce přesčas, noční práce, doby pracovní pohotovosti, kterou zaměstnanec pracoval a doby pracovní pohotovosti, kterou zaměstnanec držel.[280] Když zaměstnavatel tuto povinnost řádně neplní, jedná se dokonce o přestupek ve smyslu zákona č. 251/2005 Sb., o inspekci práce.[281] Na straně druhé této evidenční povinnosti zaměstnavatele odpovídají také různé povinnosti zaměstnance, především pak jeho povinnost být na začátku pracovní směny na svém pracovišti a odcházet z něj až po jejím skončení.[282] Stejně jako neplnění evidenční povinnosti u zaměstnavatele má své negativní důsledky v podobě rizika uložení pokuty, i u zaměstnance platí, že pokud tuto svou povinnost řádně nedodržuje, může takové jednání vést až ke skončení pracovního poměru.[283]

Zaměstnavatelé historicky tuto svou povinnost, která jim zároveň umožňuje kontrolovat, zda zaměstnanci řádně plní své pracovní povinnost, kontrolovali různými způsoby. Od zápisů na vrátnici přes používání klasických „píchaček“ až po přidělování elektronických karet, které jsou přiděleny konkrétnímu zaměstnanci, kdy taková karta umožňuje vstup do budovy a zároveň eviduje okamžik vstupu i odchodu. Stejně jako u všech ostatních oblastí, kterým se tato práce věnuje, i zde platí, že používání biometrických technologií, v jejichž důsledku zaměstnavatelé zpracovávají biometrické údaje svých zaměstnanců, bude pravděpodobně stále oblíbenější. Důvodů pro takový postup je hned několik.

Tím hlavním přitom je, že všechny z výše popsaných způsobů evidence pracovní doby jsou náchylné k určité úrovni chybovosti a nepřesnosti. Ať už bude tato způsobena přímo snahou zaměstnance, který například hekne přidělenou kartičku k evidenci své docházky nebo například vnějšími vlivy jako její ztrátou či krádeží, nelze vyloučit, že bude mít zaměstnavatel

[279] Srov. technologie dostupné v oblasti biometrické ochrany přístupů na trhu od společnosti Nedap. [dostupné online na nedapsecutiry.com].
[280] Srov. ustanovení § 96 zákoníku práce.
[281] Srov. ustanovení § 15 odst. 1 písm. l) citovaného zákona.
[282] Srov. ustanovení § 81 odst. 3 zákoníku práce.
[283] Srov. ustanovení § 52 a § 55 zákoníku práce.

s takovým způsobem evidence pracovní doby poměrně vysoké náklady a značnou administrativní zátěž. Používání biometrických údajů, jako například skenu obličeje či otisku prstu, však většinu všech negativních externalit ostatních způsobů evidence docházky zaměstnance v podstatě eliminuje. Otisk prstu nelze nijak zfalšovat, nelze jej ztratit ani si nechat ukrást a je zde dána kompletní jistota, že se na pracoviště vždy skutečně osobně dostaví ten který konkrétní zaměstnanec. Taková biometrická technologie je přitom často nastavena tak, že umožňuje zaměstnavateli konkrétně identifikovat každého jednotlivého zaměstnance a umožnit mu přesně určit, kdy daný zaměstnanec do práce přišel, kdy odešel, kdy v ní být z důvodu dovolené či dočasné pracovní neschopnosti nemá atd.

Jako u všech ostatních typů zpracování biometrických údajů ze strany zaměstnavatele i v tomto případě platí, že se bude jednat o zpracování zvláštní kategorie osobních údajů a uplatní se tak omezení podle čl. 9 Nařízení. Jelikož v práci bylo již výše vysvětleno, že v praxi obecně fungujícími právními tituly pro takové zpracování ze strany zaměstnavatele budou čl. 9 odst. 2 písm. a) a písm. b) Nařízení, nebude tomu jinak ani v tomto případě. Jak bylo opakovaně zmíněno, výslovný souhlas je přitom vždy problematický ve vztazích, kde panuje určité nerovné postavení, což mezi zaměstnanci a zaměstnavateli jednoznačně je.[284] Určitým návodem, kdy bude možné zpracování biometrických údajů pro docházkové systémy používat, potom je případ výše i níže zmíněné kontroly ze strany ÚOOÚ provedené u společnosti Metrostav.[285] Každý zaměstnavatel, který bude chtít tímto způsobem postupovat, však musí mít na paměti, že tak lze učinit pouze v případě naprosto specifických okolností, kdy jednak splní do důsledku všechny ostatní povinnosti dle Nařízení, jednak u něj evidence docházky např. nebude proveditelná jiným způsobem.

6.2.4. Prostředky zaměstnavatele používané k výkonu práce

Když se v této práci mluví o prostředcích zaměstnavatele používaných k výkonu práce, nemyslí se tím *terminus technicus* osobních ochranných pracovních prostředků ve smyslu § 104 zákoníku práce, ale v podstatě všechny hmotné, ale i nehmotné statky, které zaměstnavatel poskytuje či zpřístupňuje svým zaměstnancům za účelem výkonu jejich práce. Může se tak jednat například o služební automobil, služební telefon či počítač, dále například stroje

[284] V úvahu připadá užití docházkových systémů na biometrické bázi s výslovným souhlasem zaměstnance opětovně v případě, že zaměstnanci budou mít k takové evidenci určitou alternativu.
[285] Srov. Kontrola používání technologie FaceID (společnost Metrostav a.s.). [dostupné online z uoou.cz]. Úřad pro ochranu osobních údajů. 2018.

a výrobní zařízení v továrnách, ale také například speciální software či jakékoli digitální rozhraní, které zaměstnanec speciálně používá k výkonu své práce.

U zmíněných hmotných prostředků nebude užívání biometrických technologií (snad s výjimkou mobilních telefonů) natolik časté ani v dnešní době, ale pokud se nehmotných prostředků týče, jako například právě přístupu do určitého digitálního pracovního rozhraní, tak v tomto ohledu již má užití biometrických technologií smysl a je často používáno, a zaměstnavatel se tak v souvislosti s tím může dostat do role správce či zpracovatele zvláštní kategorie osobních údajů.

Asi nejběžnějším příkladem takového přístupu k prostředku poskytnutého zaměstnavatelem bude technologie, která je zabudována i v operačním systému Windows, kterou je tzv. Windows Hello. Tento program je možné používat k přihlášení na určitý pracovní prostředek, ale i do konkrétního softwarového rozhraní, a to několika odlišnými způsoby. Mezi těmi je mj. možné zvolit i nastavení přístupu přes zpracování biometrických údajů přihlašovaného, tedy zaměstnance, konkrétně například sken obličeje či čtečku otisku prstů. Tento postup je v rámci Windows Hello uživatelsky nejméně náročný, nejrychlejší a také poskytuje nejvyšší stupeň ochrany pro všechny zúčastněn subjekty. Všechny tyto benefity pak pochopitelně vedou k závěru, že i v rámci užívání pracovních prostředků budou zaměstnavatelé stále častěji požadovat, aby se zaměstnanci identifikovali prostřednictvím biometrických údajů, které je jednak velmi obtížné zfalšovat, jednak je v podstatě nelze žádným způsobem odcizit. Ve zbytku jsou pro tuto podkapitolu použitelné závěry i z podkapitoly předchozí týkající se řízení přístupu.

6.2.5. Ostatní činnost zaměstnavatele

Kromě již řečených oblastí, ve kterých bude v rámci pracovněprávních vztahů docházet ke zpracování biometrických údajů, již v dnešní době nejčastěji existují i jiné činnosti prováděné zaměstnavatelem, u kterých si lze používání biometrických technologií a zpracování biometrických údajů v budoucnu představit.

Mezi tyto je možno zařadit například oblast péče o zaměstnance, především pak ve vztahu k jejich odbornému rozvoji, lepší zajištění bezpečnosti a ochrany zdraví při práci související s právní úpravou pracovních úrazů a nemocí z povolání či například odměňování a náhrada výdajů vzniklých zaměstnanci v případě výkonu práce pro zaměstnavatele. Ve všech těchto oblastech si lze představit, že v budoucnu nebudou fungovat na základě složitých

evidencí, výpisů z účtů, záznamů o školení, potvrzení o účasti na výuce a dalších listinách, které s sebou přináší poměrně zásadní administrativní zátěž, ale že všechny tyto pracovněprávní instituty budou součástí jakéhosi celkového profilu zaměstnance, který bude jak z jeho strany, tak ze strany zaměstnavatele pravidelně aktualizován právě používáním biometrických údajů.

Jako jeden příklad za všechny v tomto ohledu lze označit například kamerový systém fungující v provozu, kde je velký hluk a obecně nepříznivé prostředí (vysoké teploty, nebezpečné nástroje a další), kdy zároveň zaměstnanci nad sebou nemají dohled navzájem, tj. pracují u jednotlivých přístrojů odděleně. Takový kamerový systém může být totiž již v dnešní době vybaven vnímáním tělesné termoregulace, snímačem tepové frekvence a dalších údajů o konkrétním zaměstnanci, které budou biometrické povahy a na jejichž základě bude možné konkrétního zaměstnance vždy identifikovat, pročež zaměstnavatel bude v důsledku použití takového systému správcem osobních údajů. Účelem by však v takovém případě bylo jednak obecné dodržování bezpečnosti a ochrany zdraví při práci, ke kterému byli zaměstnanci řádně proškoleni, jednak předcházení fatálním pracovním úrazům, neboť takový software by například mohl vždy upozornit vedoucího pracovníka dané směny, pokud by u některého ze zaměstnanců došlo k vážnému zranění.

Přestože by se dalo zpracování biometrických údajů použít vesměs k pozitivním účelům, které z podkapitol této části vyplývají, bude v budoucnu nutné při přípravě nové legislativy pamatovat také na skutečnost, že jsou biometrické údaje lehce zneužitelné a že jsou skutečně velmi citlivé povahy. I když tedy současný stav, kdy zaměstnavatelé mohou zpracovávat biometrické údaje jen velmi výjimečně, nelze označit za ideální, bude nutné k vytvoření lepšího legislativního rámce do budoucna přistupovat s maximální opatrností.

6.3. Další vývoj

Jak plyne ze shora uvedeného, oblastí, ve kterých dochází a v budoucnu bude stále častěji docházet ke zpracování biometrických údajů v pracovněprávních vztazích, existuje skutečně mnoho. Navzdory tomu však neexistuje v současné době žádná exaktní právní úprava, která by se této problematice zevrubněji věnovala. To přesto, že Nařízení je účinné již více než tři roky a že zrovna do oblasti zpracování biometrických údajů vneslo spíše nejasnosti a nejistoty v tom, jak a za jakých okolností lze biometrické údaje obecně, natož pak v pracovněprávních vztazích, zpracovávat.

Že je oblast biometrických technologií obecně na vzestupu, plyne i z toho, jakým způsobem se užívání biometriky podílí na našem každodenním životě. Biometrickou technologii dneska obsahují v podstatě všechny smart telefony, které se logují na základě snímání obličeje či čtečky otisku prstu. V bankovním sektoru v České republice už téměř polovina finančních institucí používá biometrické technologie pro komunikaci a zjednodušení smluvních procesů se svými zákazníky.[286] Již patnáct zemí pouze z Evropské unie pravidelně používá ke sledování veřejného prostoru biometrické prostředky spočívající v automatickém rozpoznávání obličejových identifikátorů.[287] A celosvětový obrat ve vztahu k biometrických technologiím v rozmezí let 2017 až 2025 každoročně poroste téměř o 20 %.[288]

Jakým způsobem se potom k jejich zpracování v budoucnu postaví ÚOOÚ, lze jen těžko předpovídat. V pracovněprávních vztazích může jako jakýsi návod posloužit připomínka ÚOOÚ k novele zákoníku práce, jež byla aktuální v roce 2019.[289] V tomto dokumentu ÚOOÚ uvedl, že reaguje na novelu zákoníku práce a zákona o zaměstnanosti v oblasti biometrických údajů proto, že se jedná o společenský problém, jehož incidence i prevalence vykazuje rostoucí trend, neboť biometrická identifikace je v České republice zaměstnavateli hojně používána. Z tohoto důvodu navrhl ÚOOÚ znění nového § 316a zákoníku práce, které mělo následující textaci:

> *(1) Zaměstnavatel může využívat k ochraně svých výrobních a pracovních prostředků a technologií biometrické údaje identifikující zaměstnance a používající pouze morfologické znaky zaměstnanců.*
>
> *(2) Tyto údaje lze využívat pouze pro kontrolu přístupu k výrobním a jiným provozním zařízením zaměstnavatele a vstupu do objektů zaměstnavatele nebo jejich částí kde jsou taková zařízení umístěna.*
>
> *(3) Pro účely podle odstavce 1 a 2 lze zpracovávat pouze v rozsahu nezbytném*
>
> *a) identifikační údaje zaměstnanců*

[286] POKORNÝ, M. *Z biometrických dat používají české finanční instituce nejčastěji digitální podpis a rozeznávání hlasu*. [dostupné online na techfocus.cz]. Techfocus. 2020.
[287] MACH, J., VOBOŘIL, J. *Využití biometriky při sledování veřejného prostoru v České republice*. [dostupné online na digitalnisvobody.cz]. Iuridicum Remedium. Digitální svobody. 2021.
[288] KŘÍŽ, L. *Biometrická řešení: Trh poroste*. [dostupné online na Businessworld.cz]. Businessworld. 2020.
[289] Připomínka ÚOOÚ z 29. července 2019, č. j. UOOU-02950/19-4 k návrhu zákona, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů.

b) provozní údaje technického zařízení využívaného k biometrické identifikaci a autentizaci zaměstnanců a

c) údaje vytvořené takovým technickým zařízením nebo za jeho pomoci.

K odůvodnění takového postupu potom ÚOOÚ uvedl, že daný krok považuje za nezbytný, a to s ohledem na znění čl. 9 Nařízení v jehož důsledku pro zpracování zvláštní kategorie osobních údajů, do které patří i údaje biometrické, nepostačuje naplnění některého ze základních právních titulů jako plnění zákonné povinnosti či oprávněný zájem zaměstnavatele, což v praxi činí nemalé potíže.[290] Začleněním § 316a do zákoníku práce tak ÚOOÚ sledoval umožnění zpracování biometrických údajů zaměstnanců za účelem ochrany výrobních a pracovních prostředků zaměstnavatele, na základě čehož by každý zaměstnavatel splňující podmínky dle komentovaného ustanovení splnil právní titul dle čl. 9 odst. 2 písm. b) Nařízení. Specificky pak ÚOOÚ zmiňuje, že je dané ustanovení koncipováno záměrně velmi restriktivně, aby například neumožňovalo zpracovávat biometrické údaje pouze za účelem evidence docházky zaměstnanců konkrétního zaměstnavatele. Z toho důvodu by součástí novely bylo stanovení jasného účelu, pro který by mohl zaměstnavatel biometrické údaje zpracovávat, jakož i okolnosti, za kterých by bylo možné takové biometrické údaje zaměstnance použít. Navíc zaměstnavatel by mohl na základě zmíněného ustanovení zpracovávat pouze tři okruhy osobních údajů svých zaměstnanců, jak stanovil navrhovaný odst. 3.

I přes tyto snahy ÚOOÚ přijatý zákon č. 285/2020 Sb., kterým se mění zákon č. 262/2006 Sb., zákoník práce účinný částečně od 30. července 2020 a částečně od 1. ledna 2021 žádnou speciální úpravu biometrických údajů neobsahuje, a ani důvodová zpráva, která byla spolu s tímto zákonem vydaná žádným způsobem oblast biometriky nezmiňuje. Jakýkoli budoucí vývoj se dá tak odhadovat z rozhodovací praxe ÚOOÚ, která již byla částečně nastíněna v předchozí části této kapitoly, kde byla ve větší podrobnosti pojednáno o identifikaci FaceID, kterou používala společnost Metrostav.[291] V daném rozhodnutí ÚOOÚ dospěl k závěru, že společnost Metrostav neporušila žádnou povinnost stanovenou Nařízením, když zpracovávala biometrické údaje svých zaměstnanců (sken obličeje) za účelem jejich identifikace na některých staveništích a za účelem umožnění přístupu na tyto staveniště, kdy jako právní titul pro jejich zpracování ÚOOÚ posoudil čl. 9 odst. 2 písm. b) Nařízení.

[290] Srov. čl. 6 odst. 1 písm. c) a písm. f) Nařízení.
[291] Srov. Kontrola používání technologie FaceID (společnost Metrostav a.s.). [dostupné online z uoou.cz]. Úřad pro ochranu osobních údajů. 2018.

Důležitým faktorem v jeho rozhodnutí také bylo, že společnost Metrostav plnila všechny ostatní povinnosti zaměstnavatele coby správce osobních údajů v souladu s Nařízením a že daného cíle nemohla dosáhnout jiným způsobem. Lze tak očekávat, že za splnění určitých podmínek bude ÚOOÚ k užívání biometrických údajů mít přístup spíše praktický.

V částečně opačném taktu (i když mimo pracovněprávní oblast) pak hovořilo rozhodnutí ÚOOÚ ve věci užití tzv. dynamických biometrických podpisů ze strany finanční instituce u svých klientů/spotřebitelů, kdy ÚOOÚ rozhodl,[292] že zpracování biometrických údajů v důsledku užití této technologie není průchozí přes tzv. balanční test[293] a je v rozporu s principem přiměřenosti zpracování osobních údajů.[294] I když bylo toto rozhodnutí ÚOOÚ odbornou veřejností poměrně velmi kritizováno,[295] nelze do budoucna vyloučit, že ÚOOÚ nebude přeci jen zpracování biometrických údajů otevřen natolik, jak by se mohlo na první pohled zdát. Rozhodující budou každopádně vždy skutkové okolnosti daného případu a v rámci pracovněprávních vztahů nezbývá než doufat v racionální přístup tohoto úřadu.

Z uvedeného tak plyne, že je v současné době právní rámec a vnímání zpracování biometrických údajů a užívání technologií se schopností biometrické identifikace a autentizace konkrétních subjektů velmi vágní. Po Nařízení není žádných pochyb o tom, že biometrické údaje jsou tzv. zvláštní kategorií osobních údajů a že k jejich zpracování je nutné naplnit jeden z právních titulů dle čl. 9 odst. 2 Nařízení. Jak je naznačeno v této kapitole shora, v oblasti pracovněprávních vztahů přitom splnění této povinnosti ze strany zaměstnavatele coby správce osobních údajů není vůbec jednoduché, neboť téměř každý z právních titulů pro zpracování biometrických údajů je z nějakého důvodu problematický. Ty dva, které připadají nejvíce v úvahu, tedy zpracování na základě výslovného souhlasu[296] a z důvodu plnění povinností[297] narážejí v prvním případě na problém odvolatelnosti a skutečnost, že zaměstnanec je ve vztahu k zaměstnavateli vždy v nerovném postavení, a v druhém případě na to, že vedle splnění právního titulu musí vždy správce splnit i všechny ostatní povinnosti dle Nařízení, mezi které

[292] Rozhodnutí ÚOOÚ z 21. března 2019, č. j. UOOU-10138/18-8.
[293] Balanční test se užívá při užití právního titulu dle čl. 6 odst. 1 písm. f) Nařízení, kdy je správce osobních údajů pro zachování principu přiměřenosti vždy povinen zkoumat a poměřovat (i) svůj oprávnění zájem, (ii) nezbytnost zpracování a (iii) zájmy a základní práva a svobody subjektu údajů, jak je uvedeno např. v RÁMIŠ, V. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 6 Nařízení.
[294] Srov. čl. 5 odst. 1 písm. c) Nařízení.
[295] MAISNER, M., SMEJKAL, V., UŘIČAŘ, M. in *Je používání dynamického biometrického podpisu v rozporu s GDPR?* [dostupné online na epravo.cz]. Epravo. 2019.
[296] Srov. čl. 9 odst. 2 písm. a) Nařízení.
[297] Srov. čl. 9 odst. 2 písm. b) Nařízení.

patří mj. i přiměřenost jejich zpracování, což u biometrických údajů často nebude naplněno. Jak totiž uvádí komentářová literatura, jsou typické příklady, ve kterých bude možné zpracování na základě čl. 9 odst. 2 písm. b) použít v podstatě vždy (jako například údaje o zdravotním stavu zaměstnanců,[298] kdy naopak u jiných povinností dle zákoníku práce (typicky evidence docházky dle § 96 zákoníku práce) nebude možné zpracování na základě tohoto právního titulu bez dalšího použít.

V kontextu právě řečeného tak není žádných pochyb o tom, že idea ÚOOÚ o potřebě upravit zpracování osobních údajů přímo v zákoníku práce nebyla ve své podstatě špatným legislativním nápadem, neboť by zaměstnavatelům v této oblasti poměrně zásadně rozvazoval ruce. To vše platí o to víc, že se nacházíme v době možná největšího technologického rozmachu v historii lidstva, a zatímco FaceID či čtečka otisku prstů byla před několika lety součástí jen těch nejlepších mobilních telefonů na trhu, dnes už tyto technologie používá v podstatě každý. V tomto kontextu dává perfektní smysl, aby i zaměstnavatelé měli ve shora nastíněných oblastech možnost používat biometrické technologie autentizace a identifikace svých zaměstnanců vedoucí ke zpracování jejich osobních údajů, a to bez jakéhokoli zásadního rizika postihu ze strany úřadů kontrolující ochranu osobních údajů.

[298] OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021. Komentář k čl. 9 Nařízení.

7. Závěr

Účelem této rigorózní práce bylo zevrubně pojednat o problematice ochrany osobních údajů se zaměřením na pracovněprávní vztahy s aplikací tzv. biometriky. Zpracování biometrických údajů a s tím související právní aspekty sice nejsou ve světě vědy ničím novým a neprobádaným, nicméně s ohledem na stále dostupnější technologické výdobytky dnešní doby lze očekávat, že se i přesto bude v následujícím období jednat o jedno z ústředních témat, kde se bude pravidelně setkávat problematika ochrany osobních údajů s pracovním právem.

Ve snaze o řádné uchopení ústředního tématu této práce se nejdřív v první části věnujeme zevrubné deskripci hlavních terminologických pojmů právní úpravy ochrany osobních údajů vůbec a následně práv a povinnosti všech subjektů, které v rámci ochrany osobních údajů vznikají, ať už se jedná o práva a povinnosti správce či zpracovatele či práva a povinnosti subjektu údajů. Hlavním záměrem této části bylo vyjasnit a deskriptivně ukotvit všechny pojmy a všechny rozhodující a stěžejní procesy v rámci zpracování ochrany osobních údajů takovým způsobem, aby již v částech následujících nemohlo docházet k žádným zásadním výkladovým problémům. Vzhledem k tomu, že Nařízení je jednak již několik let aplikováno v praxi, jednak spoustu matérie převzalo ze Směrnice coby svého předchůdce, existuje ke správnému uchopení všech stěžejních institutů ochrany osobních údajů velké množství relevantní literatury, a to zejména s ohledem na práci pracovní skupiny WP 29 a Evropského sboru pro ochranu osobních údajů. Zejména díky těmto dvěma organizacím a jejich výkladovým stanoviskům v dnešní době většina základních pojmů a teleologických východisek ochrany osobních údajů nečiní v aplikační praxi větší potíže, z čehož do značné míry čerpala rovněž tato práce. Ani přesto však nelze opomenout některé problematické aspekty Nařízení, kdy tím možná úplně nejzásadnějším ve světle této stati je poněkud nešťastně zvolená definice biometrického údaje.

V následující části se práce již konkrétněji zaměřila na to, jaká jsou specifika ochrany osobních údajů v pracovněprávních vztazích. Samotné Nařízení totiž v několika svých pasážích oblast pracovního práva (ale i práva sociálního zabezpečení) staví na speciální místo a počítá pro účely těchto právních odvětví se zvláštní úpravou v rámci jednotlivých členských států. Podstatné zejména je, aby si jak zaměstnavatelé, tak zaměstnanci vždy uvědomovali, že ke zpracování osobních údajů dochází z mnoha různých důvodů, přičemž se vždy nemusí jednat pouze o plnění zákonné povinnosti zaměstnavatele, a že ke zpracování nemusí docházet pouze v rámci již existující pracovního poměru, ale také v případě náborových řízení, nebo dokonce

i po řádném skončení pracovního poměru. Po celou tuto dobu se přitom na všechny zúčastněné vztahují všechna práva a povinnosti z Nařízení vyplývající. Již v této části bylo zároveň naznačeno, jakým způsobem a v jakých fázích může v rámci pracovněprávních vztahů docházet ke zpracování právě biometrických údajů. Důvodem, proč jsou pracovněprávní vztahy a využívání biometriky relativně hodně provázané, je zejména spolehlivost a jen těžko představitelná zneužitelnost biometrických údajů. Díky jejich používání je totiž zaměstnavatel zpravidla schopen efektivnějšími a administrativně méně náročnými procesy plnit řadu svých povinností nejen dle Nařízení coby správce osobních údajů, ale i dle zákoníku práce coby zaměstnavatel. Zároveň je pro zaměstnance těžké při používání jeho biometrických údajů systémy zaměstnavatele jakýmkoli způsobem obejít a zaměstnavatel tím rovněž i chrání své oprávněné, především majetkové zájmy.

S ohledem na shora uvedené se práce ve své poslední části již podrobně zaměřuje na využívání biometrických údajů v pracovněprávních vztazích v konkrétních situacích. Prvním problémem však je, že biometrické údaje dle čl. 9 Nařízení spadají do tzv. zvláštní kategorie osobních údajů, což způsobuje, že v praxi vzniká v souvislosti s jejich zpracováním ze strany zaměstnavatelů poměrně mnoho praktických potíží. Tou hlavní potom je, že zvláštní kategorie osobních údajů může správce osobních údajů zpracovávat jen na základě speciálních právních titulů ve smyslu čl. 9 odst. 2 Nařízení a v pracovněprávních vztazích se většina z nich jeví jako aplikačně nevhodná, resp. nemožná. Současně tak zpracování probíhá především na základě výslovného souhlasu, případně z důvodu ochrany oprávněných zájmu zaměstnavatele ve smyslu čl. 9 Nařízení, ale nelze s jistotou říct, že dané postupy budou bez dalšího aprobovány i orgány veřejné moci. Zaměstnavatelé tak v momentální době žijí v poměrně velké nejistotě, jaká forma zpracování biometrických údajů je a bude i v budoucnu z pohledu ÚOOÚ ještě přijatelným a přiměřeným zpracováním ve smyslu Nařízení a u jaké by již byli zaměstnavatelé za hranicí přípustných opatření a vystavovali by se tak riziku právní sankce. Jak je přitom ukázáno v této stati, oblastí, ve kterých zaměstnavatelé mohou s dnešními snadno přístupnými moderními technologiemi zpracovávat biometrické údaje svých zaměstnanců, je skutečně mnoho, a této problematice by tak měla být věnována větší pozornost. Užití biometrických údajů může totiž stranám pracovněprávního vztahu sloužit od okamžiku, kdy ještě ani nevznikl pracní poměr (např. užitím aplikací na zabránění tzv. *Identity Theft*), až do doby jeho skončení, neboť v průběhu pracovního poměru lze biometrické údaje užívat například na evidenci docházky, elektronizaci osobního spisu zaměstnance, kontrolu přístupů a další. Bohužel, jediná historická snaha zákonodárné povahy, která se na území České republiky problematice

zpracování biometrických údajů věnovala, byl záměr ÚOOÚ zavést konkrétní normotvorbu do zákoníku práce, a to konkrétně vytvořením nového § 316a. Tento záměr však s novelou zákoníku práce, která byla aktuální v letech 2016 a 2017, neprošel a nyní zde bez pochyby existuje jakési právní vakuum, které bude postupně vyplňováno až na základě *ad hoc* případů, které se budou řešit v rámci rozhodovací praxe ÚOOÚ.

O to víc platí, že do budoucna skutečně nemůže být tato oblast přehlížena takovým způsobem, jak tomu bylo doposud. Zpracování biometrických údajů je totiž v dnešní době již součástí našeho každodenního života, neboť s nimi pracujeme nejen například v rámci finančního sektoru, ale mj. úplně pokaždé, když vezmeme do ruky mobilní telefon. Není proto nejmenší důvod k tomu, aby natolik svébytná oblast, která se dotýká většiny ekonomicky aktivních osob žijících v České republice, jakou je pracovní právo, byla v tomto ohledu i nadále neprobádanými vodami. To proto, že je zde na straně jedné potřeba nastolení větší právní jistoty a na straně druhé také nutnost znova se přizpůsobit a o něco více přiblížit moderním trendům a technologiím, které v mnoha oblastech mohou každodenní zejména administrativní zátěž velice zjednodušit. Již jen na základě uvedených důvodů je oblast biometriky v pracovněprávních vztazích velmi aktuálním tématem, kterému by měla být v legislativních kruzích věnována větší pozornost.

SEZNAM POUŽITÝCH ZKRATEK

ESLP – Evropský soud pro lidská práva;
Nařízení – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;
LZPS – Listina základních práv a svobod;
NS – Nejvyšší soud;
NSS – Nejvyšší správní soud;
OZ – zákon č. 89/2012 Sb., občanský zákoník;
SDEU – Soudní dvůr Evropské unie
Směrnice – Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;
ÚOOÚ – Úřad pro ochranu osobních údajů;
Zákoník práce – zákon č. 262/2006 Sb., zákoník práce;
ZOOÚ – zákona č. 101/2000 Sb., o ochraně osobních údajů;
ZOZOÚ – zákon č. 110/2019 Sb., o zpracování osobních údajů.

SEZNAM POUŽITÝCH ZDROJŮ

1. Seznam použité literatury

BĚLINA, M., DRÁPAL, L. a kol.: *Zákoník práce. Komentář.* 3. vydání. Praha: C. H. Beck. 2019;

BREJCHOVÁ, D. in UŘIČÁŘ, M., RÁMIŠ, V., a kol.: *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021;

JANŠOVÁ, M. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář*. 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020;

JELÍNEK, T. in VALENTOVÁ, K., PROCHÁZKA, J., JANŠOVÁ, M., ODROBINOVÁ, V., BRŮHA, D. a kol. *Zákoník práce. Komentář*. 1. vydání (1. aktualizace). Praha: C. H. Beck. 2020;

KOCOUREK, J., DOBŘICHOVSKÝ, T. *Pracovní právo. Vybraná ustanovení zákoníku práce. Komentář*. 1. vydání. Praha: C. H. Beck. 2020;

KUČEROVÁ, A., NOVÁKOVA, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2012;

MATEJKA, J.,, KRAUSOVÁ, A., GÜTTLER, V. *Biometrické údaje a jejich právní režim* in *Revue pro právo a technologie*. Vydání č. 17/2018. 2018;

MATEJKA, J., MATOCHOVÁ, S., PROKEŠ, J. *Analýza biometrických údajů v kontextu obecného nařízení pro ochranu osobních údajů*. Acta Informatica Pragensia. 2019;

MORÁVEK, J. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika. 2013.

MORÁVEK, J. *Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy*. Praha: Wolters Kluwer ČR. 2019;

MORDINI, E., TZOVARAS, D., (eds.). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer Netherlands. 2012;

NULÍČEK, M., DONÁT, J., NONNEMANN, F., LICHNOVSKÝ, B., TOMÍŠEK, J. *GDPR. Obecné nařízení o ochraně osobních údajů.* Praha: Wolters Kluwer. 2017;

OTEVŘEL, R. in. UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021;

POSPÍŠIL, D. in KUČEROVÁ, A., NOVÁKOVA, L., FOLDOVÁ, V., NONNEMANN, F., POSPÍŠIL, D.: *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2012;

RAK, R., MATYÁŠ, V., ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, a.s. 2008;

RÁMIŠ, V. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021;

SMEJKAL V. *Kryptografický a dynamický biometrický podpis podle platné právní úpravy*. Právní rozhledy 10/2019;

UŘIČÁŘ, M. in UŘIČÁŘ, M., RÁMIŠ V. a kol. *Obecné nařízení o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck. 2021;

WINTR, J.: *Principy českého ústavního práva*. 2. vydání. Plzeň: nakladatelství Aleš Čeněk. 2013.

2. Seznam použitých právních předpisů

Listina základních práv a svobod;

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES;

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;

Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu;

Zákon č. 263/2016 Sb., atomový zákon;

Zákon č. 89/2012 Sb., občanský zákoník;

Zákon č. 586/1992 Sb., o daních z příjmů;

Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích);

Zákon č. 101/2000 Sb., o ochraně osobních údajů;

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti;

Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení;

Zákon č. 592/1992 Sb., o pojistném na všeobecném zdravotním pojištění;

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;

Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací;

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 435/2004 Sb., zákon o zaměstnanosti;

Zákon č. 262/2006 Sb., zákoník práce.

3. Seznam použité judikatury a správních rozhodnutí

Nález Ústavního soudu České republiky ze dne 9. března 2004, sp. zn. Pl. ÚS 38/02;

Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 3. října 2008, č. j. SKO-0629/07;

Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. března 2013, č. j. SKO-2077/07;

Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. března 2019, č. j. UOOU-10138/18-8;

Rozsudek Evropského soudu pro lidská práva ve věci Amann v. Švýcarsko ze dne 16. února 2000, č. 22298/95;

Rozsudek Evropského soudu pro lidská práva ve věci Niemietz v. Německo ze dne 16. prosince 1992, č. 13710/88

Rozsudek Nejvyššího správního soudu ze dne 12. února 2009, sp. zn. 9 As 34/2008;

Rozsudek Nejvyššího správního soudu ze dne 30. ledna 2013, č. j. 7 As 150/2012-35;

Rozsudek Nejvyššího správního soudu ze dne 28. června 2013, č. j. 5 As 1/2011-156;

Rozsudek Nejvyššího správního soudu ze dne 27. února 2014, č. j. 4 As 132/2013-25;

Rozsudek Nejvyššího správního soudu ze dne 20. srpna 2014, sp. zn. 6 As 144/2013-34;

Rozsudek Nejvyššího správního soudu ze dne 25. února 2015, sp. zn. 1 As 113/2012;

Rozsudek Nejvyššího správního soudu ze dne 20. prosince 2018, sp. zn. 6 As 168/2018;

Rozsudek Soudního dvora ze dne 6. listopadu 2003 ve věci C-101/2001 (Lindqvist);

Rozsudek Soudního dvora Evropské unie ze dne 13. května 2014 ve věci C-131/12 (Google Inc. vs. AEPD);

Rozsudek Soudního dvora Evropské unie ze dne 20. října 2016 ve věci C-582/14 (Patrick Breyier vs Bundesrepublich Deutschland);

Rozsudek Soudního dvora Evropské unie ze dne 10. července 2018 ve věci C-25/17 (Jehovan Todistajat);

Rozsudek Soudního dvora Evropské unie ze dne 5. června 2018 ve věci C-210/16 (Facebbok Fan Page).

4. Seznam použitých internetových zdrojů

ČTK, IDNES.cz: *Třetina zaměstnanců pracuje podle průzkumu z domova, část z nich ruší rodina.* [dostupné online na idnes.cz]. Idnes. 2020;

CHLÁDKOVÁ, A. *Osobní údaje v pracovněprávních vztazích – Změní se něco podle GDPR.* [dostupné online na praceamzda.cz]. Práce a mzda. 2018;

JAROSLAV, D. *Jak by měl zaměstnavatel naložit s osobními údaji neúspěšných, ale přesto potenciálně zajímavých uchazečů o zaměstnání.* [dostupné online na pravniprostor.cz]. Právní prostor. 2019;

Kontrola používání technologie FaceID (společnost Metrostav a. s.). [dostupné online z uoou.cz]. Úřad pro ochranu osobních údajů. 2018;

KŘÍŽ, L. *Biometrická řešení: Trh poroste*. [dostupné online na Businessworld.cz]. Businessworld. 2020;

KUBÍČKOVÁ, A., PATÁKOVÁ, V. *Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z.* [dostupné online na praceamzda.cz]. Práce a mzda. 2017;

MACH, J., VOBOŘIL, J. *Využití biometriky při sledování veřejného prostoru v České republice*. [dostupné online na digitalnisvobody.cz]. Iuridicum Remedium. Digitální svobody. 2021;

MAISNER, M., SMEJKAL, V., UŘIČAŘ, M. in *Je používání dynamického biometrického podpisu v rozporu s GDPR?* [dostupné online na epravo.cz]. Epravo. 2019;

NONNEMANN, F. *Privacy by design jako jedno z nových pravidel pro zpracování osobních údajů?* [dostupné online na epravo.cz]. Epravo. 2018;

OMALE, G. *Gartner Predicts Increased Adoption of Mobile-Centric Biometric Authentification and Saas-Delivered IAM*. [dostupné online z Gartner.com]. Gartner. Egham, Velká Británie. 2019;

POKORNÝ, M. *Z biometrických dat používají české finanční instituce nejčastěji digitální podpis a rozeznávání hlasu*. [dostupné online na techfocus.cz]. Techfocus. 2020;

SHAM, S. *What is Identity Proofing?* [dostupné online z okta.com]. OKTA. 2019;

SPATARO, J.: *Remote work trend report: meetings*. [dostupné online z microsoft.com]. Microsoft;

ŠKUBAL, J., VEJSADA D. *Elektronický personální spis*. [dostupné online na praceamzda.cz]. Práce a Mzda. 2019;

ŠTUKOVA, K.: *Česko pracuje z domova. V některých firmách až půlka zaměstnanců.* [dostupné online na idnes.cz]. Idnes. 2020;

Zaměstnavatel jako správce osobních údajů. [dostupné online na uoou.cz]. Úřad pro ochranu osobních údajů. 2013.

5. Seznam ostatní zdrojů

Dokument Úřadu pro ochranu osobních údajů k povinnosti správců provádět posouzení vlivu na ochranu osobních údajů ze dne 8. února 2019;

Doporučení Rady Evropy č. CM/Rec (2010)13;

Doporučení Rady Evropy č. CM/Rec(2015)5;

Doporučení pracovní skupiny WP 29 ze dne 3. října 2017 – Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení;

FEDERAL TRADE COMMISION, CONSUMER SENTINEL NETWORK. *Data Book 2020*. 2021;

Pokyny Evropského sboru pro ochranu osobních údajů č. 05/2020. 2020;

Pokyny pracovní skupiny WP 29 ze dne 3. října 2017, č. WP251rev.01 k automatizovanému individuálnímu rozhodování a profilování pro účely Nařízení;

Pokyny pracovní skupiny WP 29 ze dne 28. listopad 2017 ve znění z 10. dubna 2018, č. WP259 rev.01 k souhlasu podle Nařízení;

Pokyny Evropského sboru pro ochranu osobních údajů ze dne 4. května 2020, č. 05/2020 k souhlasu podle Nařízení;

Pokyny Evropského sboru pro ochranu osobních údajů ze dne 29. ledna 2020, č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky;

Pokyny Evropského sboru pro ochranu osobních údajů ze dne 14. ledna 2021, č. 01/2021;

Pokyny pracovní skupiny WP29 ze dne 29. listopadu 2017 ve znění z 11. dubna 2018, č. 17/CS, WP260 rev.01 k transparentnosti podle Nařízení;

Pokyny pracovní skupiny WP29 ze dne 4. dubna 2017 ve znění z 4. října 2017, č. WP 248 rev. 01 pro posouzení vlivu na ochranu údajů a stanovení, zda *„je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*“ pro účely Nařízení;

Pokyny pracovní skupiny WP29 ze dne 5. dubna 2017, č. WP242 rev. 01 týkající se práva na přenositelnost údajů;

Připomínka Úřadu pro ochranu osobních údajů z 29. července 2019, č. j. UOOU-02950/19-4 k návrhu zákona, kterým se mění zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů;

Stanovisko Evropského sboru pro ochranu osobních údajů ze dne 4. května 2020, č. 5/2020 k souhlasu dle Nařízení;

Stanovisko Úřadu pro ochranu osobních údajů č. 7/2002. 2002, 2005, 2009;

Stanovisko Úřadu pro ochranu osobních údajů č. 3/2009. 2009;

Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009. 2009, aktualizace 2014;

Stanovisko Úřadu pro ochranu osobních údajů č. 2/2011. 2011, aktualizace 2014;

Stanovisko Úřadu pro ochranu osobních údajů č. 3/2011. 2011;

Stanovisko Úřadu pro ochranu osobních údajů č. 4/2012. 2012;

Stanovisko Úřadu pro ochranu osobních údajů č. 4/2013. 2013;

Stanovisko Úřadu pro ochranu osobních údajů č. 3/2014. 2014;

Stanovisko Úřadu pro ochranu osobních údajů č. 1/2017. 2018;

Stanovisko pracovní skupiny WP 29 č. 10/2004. 2004;

Stanovisko pracovní skupiny WP 29 č. 5/2005, (WP 115), o používání lokalizačních údajů. 2005;

Stanovisko pracovní skupiny WP 29 č. 4/2007 (WP 136). 2007;

Stanovisko pracovní skupiny WP 29 (WP 80), o biometrice. 2003;

Stanovisko pracovní skupiny WP29 č. 1/2010 (WP 169). 2010;

Stanovisko pracovní skupiny WP 29 č. 10/2004. 2004;

stanovisko pracovní skupiny WP 29 č. 15/2011 (WP 187), k definici souhlasu. 2011;

Stanovisko pracovní skupiny WP 29 č. 3/2012 (WP 193). 2012;

Stanovisko pracovní skupiny WP 29 č. 2/2013. 2013;

Stanovisko pracovní skupiny WP29 č. 3/2013, k účelovému omezení. 2013;

Stanovisko pracovní skupiny WP 29 2014 č. 6/2014 (WP 217), k pojmu oprávněných zájmů podle Směrnice. 2014;

Stanovisko pracovní skupiny WP29 č. 5/2014 (WP216), k technikám anonymizace. 2014;

Stanovisko pracovní skupiny WP 29 č. 6/2014 (WP 217), k pojmu oprávněných zájmů podle Směrnice. 2014;

Stanovisko pracovní skupiny WP 29 č. 2/2017 (WP 249), ke zpracování osobních údajů na pracovišti. 2017;

Stanovisko pracovní skupiny WP 29 č. WP 248 rev.01. 2017;

Vodítko pracovní skupiny WP 29 ze dne 3. října 2017 k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení, (WP250).

OCHRANA OSOBNÍCH ÚDAJŮ PODLE GDPR SE ZAMĚŘENÍM NA PRACOVNĚPRÁVNÍ VZTAHY A BIOMETRIKU

ABSTRAKT

Tato rigorózní práce se věnuje velmi komplexní a právně složité problematice ochrany osobních údajů v období od nabytí účinnosti GDPR, tedy od května 2018 nadále. Přijetí tohoto nařízení o ochraně osobních údajů lze jistě označit za jeden z nejvíce zlomových momentů v historii evropského zákonodárství, neboť nikdy předtím neexistoval natolik rozsáhlý unifikační předpis, který by všechny členské státy donutil takto svébytnou oblast regulovat naprosto stejným způsobem. Již jen z toho důvodu se jak před nabytím účinnosti GDPR, tak po tomto okamžiku na téma ochrany osobních údajů vedou bohaté diskuze, neboť dotčené nařízení přineslo mnoho významných změn, které předtím na poli ochrany osobních údajů neměly obdoby. Účelem této statě přitom nebylo komplexně pojednat o všech těchto nových institutech, právech a povinnostech a dalších parametrech GDPR, ale zevrubně popsat pouze ty nejpodstatnější z nich a následně se zaměřit na jejich specifika v pracovněprávních vztazích, a to se zaměřením na biometriku.

Z toho důvodu se druhá část práce nejdříve věnuje tomu, v jakých situacích je zaměstnavatel povinen zpracovávat osobní údaje svých zaměstnanců nebo potenciálních zaměstnanců. To proto, že zpracování osobních údajů v rámci pracovněprávních vztahů lze rozdělit do tří samostatných časových úseků, kdy v každém z nich dochází ke zpracování jiného okruhu osobních údajů. V první řadě ke zpracování osobních údajů potenciálních zaměstnanců dochází již v rámci výběrových řízení, ve kterých zaměstnavatelé získávají informace o dotčených uchazečích za účelem nalezení toho správného kandidáta. Po skončení výběrového řízení a uzavření pracovní smlouvy následně zaměstnavatel zpracovává osobní údaje svých zaměstnanců po dobu trvání pracovního poměru, a to většinou na základě účelu plnění zákonných povinností. Zaměstnavatel totiž musí podle právních předpisů zpracovávat spoustu osobních údajů týkajících se nejen pracovního poměru a dějů, které se v něm odehrávají, ale také osobní údaje ve vztahu k daňovým a sociálním odvodům. A konečně i v případě, kdy dojde ke skončení pracovního poměru (bez ohledu na to, jakým způsobem), zaměstnavatel je podle některých zákonů povinen po určitou dobu uchovávat některou dokumentaci, jako například evidenční listy důchodového pojištění, mzdové listy a další.

Po zevrubném popisu, jakým způsobem dochází ke zpracování osobních údajů v rámci pracovněprávních vztahů, se pak již práce soustředí na poslední stěžejní oblast, a to na zpracování biometrických údajů zaměstnanců. Biometrické údaje totiž podle GDPR patří mezi tzv. zvláštní kategorii osobních údajů, což jinými slovy znamená, že se na jejich správce a zpracovatele vztahují větší povinnosti než při zpracování obyčejných osobních údajů. V dnešní moderní době je přitom využívání biometrických technologií i v rámci pracovněprávních vztahů mnohem častější, neboť to je administrativně mnohem méně náročné než tradiční způsoby zpracování osobních údajů a biometrické údaje nejdou žádným způsobem zfalšovat, nedají se ztratit, změnit atd. To z nich dělá pro zaměstnavatele a plnění jeho povinností dle zákoníku práce a dalších předpisů z oblasti práva sociálního zabezpečení mnohem atraktivnější data než osobní údaje obyčejné. V poslední pasáži této rigorózní práce je proto věnována pozornost především tomu v rámci jakých všech situací může mezi zaměstnavatelem a zaměstnancem dojít ke zpracování osobních údajů, a to vždy se zhodnocením, zda je zaměstnavatel k takovému zpracování vůbec oprávněn.

Rozhodující přitom je, že současná úprava zpracování biometrických údajů neodpovídá jejich praktickému užití, neboť jsou z legislativního hlediska v podstatě přehlíženy, což však není udržitelný stav. Do budoucna bude proto nezbytné věnovat této problematice mnohem více pozornosti na úrovní nejen akademické, ale i praktické a zákonodárné a uzpůsobit zpracování biometrických údajů tak, aby byly využitelné v aplikační praxi.

KLÍČOVÁ SLOVA
Ochrana osobních údajů
Biometrické údaje
Nařízení GDPR

PERSONAL DATA PROTECTION UNDER THE GDPR WITH FOCUS ON EMPLOYMENT RELATIONSHIP AND BIOMETRICS

ABSTRACT

This thesis focuses on the very complex and legally complicated issue of personal data protection in the period since the GDPR Directive came into force, i.e. from May 2018 onwards. The adoption of this data protection regulation can certainly be described as one of the most pivotal moments in the history of European legislation, as there has never before been a unifying regulation so extensive that it forced all Member States to regulate such a peculiar area in exactly the same way. For this reason alone, both before and after the GDPR came into force, the topic of data protection has been the subject of numerous debates, as the regulation in question has brought about many significant changes that were previously unprecedented in the field of data protection. The purpose of this work was not to comprehensively discuss all these new institutes, rights and obligations and other parameters of the GDPR, but to describe only the most important ones in detail and then to focus on their specifics in employment relations, with a focus on biometrics.

For this reason, the second part of the thesis first focuses on the situations in which an employer is obliged to process the personal data of its employees or potential employees. This is because the processing of personal data in the context of employment relationships can be divided into three separate time periods, each of which involves the processing of a different set of personal data. Firstly, the processing of personal data of potential employees already takes place in the context of selection procedures in which employers obtain information about the candidates concerned in order to find the right candidate. After the selection procedure and the conclusion of the employment contract, the employer then processes the personal data of its employees for the duration of the employment relationship, mostly for the purpose of fulfilling his legal obligations. In fact, the employer is required by law to process a lot of personal data relating not only to the employment relationship and the events that take place in it, but also personal data in relation to tax and social security contributions. Finally, even if the employment relationship is terminated (no matter how), the employer is obliged under the law to keep certain documentation, such as pension records, payroll records, etc., for a period of time given.

After a detailed description of how personal data is processed in the context of employment relations, the work then focuses on the last key area, namely the processing of biometric data of employees. According to the GDPR, biometric data belongs to the so-called special category of personal data, which in other words means that their controllers and processors are subject to greater obligations than when processing ordinary personal data. Nowadays, the use of biometric technologies is much more frequent even in the context of employment relations, because it is administratively much less demanding than traditional methods of processing personal data, and because biometric data cannot be falsified, lost, changed, etc. This makes them much more attractive data for the employer and the fulfilment of his obligations under the Labor Code and other social security law regulations than ordinary personal data. Therefore, in the last passage of this thesis, attention is paid in particular to all situations in which biometric personal data may be processed between employer and employee, always with an assessment of whether the employer is entitled to such processing at all.

The crucial point is that the current regulation of biometric data processing does not correspond to their practical use, as they are essentially overlooked from a legislative point of view, which is not a sustainable situation. In the future, it will therefore be necessary to pay much more attention to this issue not only at the academic level, but also at the practical and legislative level, and to adapt the processing of biometric data so that it is usable in application practice.

KEY WORDS

Personal data protection

Biometric data

GDPR Directive