PRÁVNÍ REŽIM INFORMAČNÍCH SYSTÉMŮ OBSAHUJÍCÍCH PERSONÁLNÍ ÚDAJE

Vladimír Šmíd

Masarykova univerzita v Brně, Žerotínovo nám. 9, 601 77 Brno, Česká republika
E-mail: smid@rect.muni.cz

Abstrakt
Na jaře 2000 nabyl účinnosti zákon č. 101/2000 Sb., o ochraně osobních údajů, který zásadně ovlivnil práva a povinnosti těch, jimž osobní údaje patří, i těch, kteří s nimi pracují. Příspěvek se zabývá vybranými otázkami vlastní aplikace této normy zejména ve vztahu k informačním systémům, které nakládají s personálními údaji zaměstnanců a osob nacházejících se právních vztazích obdobného typu.

1. Zaměstnavatelé jako správci osobních údajů

Zřejmě nebude pochyb o tom, že zaměstnavatelé nemohou svou úlohu v pracovněprávních vztazích plnit bez znalosti údajů o zaměstnancích, a to jak v průběhu doby trvání pracovněprávního vztahu, tak také před jeho vznikem i po jeho zániku. Spektrum těchto údajů může být podle druhu zaměstnavatele a odvětví, v němž působí, značně různorodé. Mezi nimi existují takové, které jsou společné všem a tvoří jistý obecný minimální základ, a na druhou stranu se zde vyskytují osobní údaje i natolik specifické, že se budou týkat pouze velice omezeného okruhu subjektů.

Úvodem zmiňovaná **nutnost vést osobní údaje zaměstnanců** nemá jen subjektivní charakter na straně zaměstnavatele. Nejméně stejný význam má i její objektivní stránka daná povinnostmi zaměstnavatele ve formě právních norem, které samozřejmě mohou být společností vynuceny pod hrozbou sankcí, včetně trestněprávních. V této souvislosti je však třeba uvést, že jak samotný zákon č. 101/2000 Sb., tak Zákoník práce neobsahuje speciální ustanovení, která by se explicitně komplexně zabývala zvláštnostmi ochrany osobních údajů v pracovněprávních vztazích.

Tyto zvláštnosti je pak třeba vyvozovat z jednotlivých ustanovení těchto i dalších speciálních norem a odpovídajícím způsobem je aplikovat. Poznamenejme však, že to není pouze problém českého právního řádu. Stejně aktuální je tato problematika rovněž v rámci Evropské unie, kde od srpna 2001 probíhají konzultace mezi Komisí a sociálními partnery (UNICE[1], UEAPME[2], BDI[3]) o ochraně osobních údajů zaměstnanců, přičemž dokument o výsledcích druhé etapy těchto konzultací byl zveřejněn teprve před několika týdny v prosinci 2002.

Již z výše uvedeného celkem přirozeně vyplývá, že **personální a související evidence** provozované zaměstnavateli v běžné situaci **spadají přinejmenším do obecného režimu zákona č. 101/2000 Sb**. To proto, že:

- zákon nerozlišuje, jakou právní formu má zaměstnavatel zpracovávající osobní údaje;

[1] Union of Industrial and Employers' Confederations of Europe
[2] European Association of Craft, Small and Medium-Sized Enterprises
[3] Bundesverband der Deutschen Industrie

- dle zákona není rozhodné, zda se údaje zpracovávají prostředky výpočetní techniky nebo jinými automatickými prostředky, případně manuálně;
- bez pochyby se v tomto případě nemůže jednat o zpracování osobních údajů, které by zaměstnavatel shromažďoval pro svou výlučnou soukromou potřebu;
- rovněž takové zpracování dat zaměstnanců alespoň zčásti nebude nahodilé, nýbrž bude vykazovat znaky systematičnosti; a
- z povahy věci není myslitelné, aby takový systém v praxi obsahoval údaje o neidentifikovaných či neidentifikovatelných osobách.

V takovém případě se pak dále bude nutně jednat o zpracování osobních údajů a zaměstnavatel se stává jejich **správcem**. Jako správce je pak zaměstnavatel povinen:

a) stanovit účel, k němuž mají být osobní údaje zpracovány;
b) stanovit prostředky a způsob zpracování osobních údajů;
c) zpracovávat pouze pravdivé a přesné osobní údaje, které získal v souladu s tímto zákonem;
d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu;
e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování;
f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, pokud zvláštní zákon nestanoví jinak;
g) shromažďovat osobní údaje pouze otevřeně a nikoliv pod záminkou jiného účelu nebo jiné činnosti;
h) nesdružovat osobní údaje, které byly získány k rozdílným účelům.

Další bezvýhradnou povinností je pak provedení **likvidace osobních údajů**, jakmile pomine účel, pro který byly osobní údaje zpracovávány, nebo na základě žádosti zaměstnance, který se tím domáhá ochrany svých práv. Zvláštní zákon (ten však dosud neexistuje) má stanovit výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení. Problém uvedeného ustanovení není v pojmu jako takovém – *„likvidace“* je přímo v zákoně definována a rozumí se jí fyzické zničení nosiče informace, fyzické vymazání nebo trvalé vyloučení z dalšího zpracování. Problematická však může být spíš konkrétní aplikace této podmínky. Asi nejjednodušší situace by mohla nastat, v případě elektronického zpracovávání dat, kde zaměstnavatel nechá jednoduše inkriminované položky z databáze vymazat. Obdobně by mohla být informace fyzicky zničena, vyskytovala-li se víceméně samostatně na papírovém dokumentu. Obtížnější interpretace nastane v případě, kdy pouze pro některé osobní údaje pominul účel zpracování a tyto se nacházejí na jedné listině s dalšími údaji, které jsou však naopak aktuální. V této situaci by bylo patrně nejvhodnější aktivní informace přenést na jiný dokument a původní listinu uložit například do takové části spisu, která nebude zaměstnavatelem nadále využívána a bude tak uchovávána pouze pro nahodile v budoucnu vzniklé potřeby tyto údaje použít. Dále svědčí zaměstnavateli další povinnost, a to jednou za kalendářní rok bezplatně, jinak kdykoli za přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace, subjektu údajů na základě písemné žádosti **poskytnout informace o osobních údajích** o něm zpracovávaných. Poznamenejme, výši takové úhrady nestanoví nikdo jiný než správce, ovšem je při tom omezen de facto skutečnými náklady nezbytnými na vyhledání, sestavení či jiné zpracování informace a na její předání či odeslání zaměstnanci. Současně je třeba zdůraznit, že z dikce uvedeného ustanovení vyplývá, že se tato povinnost vztahuje na informace *„o osobních údajích“*, nikoliv přímo na výpis těch údajů samotných. Na druhou stranu rozhodně nelze zaměstnavateli zakázat dobrovolně zaměstnanci poskytnout i kompletní přehled veškerých o něm zpracovávaných údajů. Současně se zde předpokládá písemná žádost zaměstnance, na niž zaměstnavatel musí reagovat obdobným způsobem. Až na výjimky zde ve většině případů bude moci být nahrazena klasická písemná forma

telegrafickými, dálnopisnými a zejména pak elektronickými prostředky; samozřejmě za předpokladu dostatečné důvěryhodnosti z hlediska autenticity žadatele a při zachování bezpečnosti dopravovaných zpráv.

2. Zabezpečení osobních údajů

Zákon zaměstnavateli přímo stanoví **přijetí takových opatření, aby nemohlo dojít k** neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému **zneužití osobních údajů**. Tato povinnost přitom platí i po ukončení zpracování osobních údajů, tj. například i po ukončení podnikání daného zaměstnavatele. Takovými opatřeními zákon rozumí opatření zejména technická a organizačně-právní, směřující jak proti náhodným vlivům, tak proti úmyslnému jednání vlastních zaměstnancům i jakýchkoliv jiných osob. Poznamenejme, že zákon tato opatření blíže nespecifikoval a ponechal tak prostor pouze pro metodická doporučení. Při praktické realizaci této povinnosti **z hlediska technického** bude zřejmě nutno vycházet z požadavku rozumné míry ochrany údajů. V případě písemných dokumentů za minimální takovou ochranu lze považovat uzamykatelný prostor (v případě citlivých údajů lépe trezor), včetně nastavení odpovídajících oprávnění, kdo má přístup ke klíčům od nich, respektive kdo taková oprávnění může přidělovat. V případě počítačových databází se bude jednat alespoň o autentikovaný přístup prostřednictvím individuálně přidělených hesel, případně i kryptování počítačových dat. Nikoliv nepodstatná bude pro případnou kontrolu ze strany Úřadu pro ochranu osobních údajů dokumentace k užívanému software, garance dané dodavatelem programového vybavení, stejně jako doklady o závazku mlčenlivosti u zaměstnanců dodavatele, kteří při instalaci či údržbě systému přijdou do styku s osobními údaji zaměstnanců objednatele.

Z pohledu organizačních a právních opatření je zaměstnavatel povinen stanovit kompetence jednotlivých zaměstnanců, kteří přicházejí při své práci do kontaktu s osobními údaji. V této souvislosti je třeba si uvědomit, že toto není jen problém personálních útvarů a pracovišť obdobného typu, ale že přinejmenším prakticky každý vedoucí zaměstnanec nakládá s osobními údaji svých podřízených a rovněž k těmto datům musí mít v nezbytném rozsahu přístup osoby na dalších funkcích. Zaměstnancům správce nebo zpracovatele a jiným osobám, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, pak zákon přímo ukládá, že mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném. Přestože v omezených případech by mělo být možné vyvodit tyto kompetence zaměstnanců již přímo z druhu práce v pracovní smlouvě, nejpřirozenější cestou zřejmě bude použití formy pracovního řádu, kde mohou být stanoveny povinnosti zaměstnanců na příslušných funkcích při nakládání s osobními údaji, stejně jako bližší podmínky pro nakládání s osobními údaji a rovněž kompetence v rozhodování o tomto nakládání.

Pro ještě širší okruh osob (tedy zaměstnancům správce nebo zpracovatele, popř. jiným fyzickým osobám, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a dalším osobám, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele), stanoví opět přímo zákon **povinnost mlčenlivosti**. Tato povinnost se nevztahuje pouze na osobní údaje jako takové, ale je rozšířena i na bezpečnostní opatření, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Uvedená povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací, není časově omezena a tedy je doživotní.

Připomeňme, že k výše vyjmenovaným povinnostem **není nutné pověřené zaměstnance** ani další osoby (počínaje techniky a konče kontrolními orgány či orgány činnými v trestním řízení) **žádným způsobem zavazovat**, protože tyto povinnosti se na ně vztahují přímo ze zákona s ohledem na roli, ve které vůči zpracování osobních údajů vystupují. Důležitější v tomto smyslu jsou správně nastavené kompetence ve vnitřních předpisech organizace, které mohou být provázány i se zde stanovenými pracovněprávními sankcemi za porušení mlčenlivosti a souvisejících povinností.

3. Další povinnosti zaměstnavatele

Zatímco v předchozím textu byly vesměs zmiňovány povinnosti, které je nezbytné v rámci pracovněprávních vztahů z pohledu ochrany osobních údajů splnit vždy za všech okolností a bez dalších podmínek, povinnosti dále uvedené budou mít již specifičtější charakter.

3.1 Účast a postavení zpracovatele

Nikoliv řídce v praxi nastává situace, kdy zaměstnavatel alespoň zčásti nevede personální a ně navazující evidence vlastními silami, ale pro tyto účely využívá externích subjektů; zpravidla to bude nahrazení nedostatku odbornosti zaměstnavatele či jeho zaměstnanců, respektive nedostatek vlastních kapacit pro konkrétní činnosti, přičemž nejčastějším příkladem v tomto smyslu bývá vedení a zpracování mzdové evidence pro malé organizace. Podstatné ovšem je, že v takovém případě vstupuje do dosavadního zpravidla dvoustranného vztahu **třetí subjekt, na nějž je nutné vztáhnout patřičná práva i povinnosti**. V souladu s definicí půjde o to, že **zpracovatelem** ve zmiňovaném případě bude každý subjekt, který na základě pověření správcem zpracovává osobní údaje podle tohoto zákona. V zákoně je navíc přímo stanovena forma tohoto pověření, a to smlouva, která musí být pod sankcí neplatnosti písemná. Dále v ní musí být zejména výslovně uvedeno v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá. Nezbytným předpokladem této smlouvy (opět pod sankcí neplatnosti) je, aby v ní zpracovatel poskytl dostatečné záruky o technickém a organizačním zabezpečení ochrany osobních údajů. Protože zpracovatel přichází do styku s osobními údaji v podstatě ve stejném rozsahu jako správce, vztáhnou se něj také **stejné povinnosti**. Výjimku tvoří pouze ty z nich, které již vlastně pojmově předat nelze, tj. zpracovatel, na rozdíl od správce, neurčuje účel, prostředky a způsob zpracování osobních údajů, zato přitom postupuje podle pokynů správce. Poněkud problematickou by mohla být otázka rozšíření povinností ze správce na zpracovatele, což se ovšem **obdobně nemůže vztahovat na předávání práv**. To pak ovšem znamená, že správce sice může zpracovávat osobní údaje, k nimž s ohledem na stanovené zákonné výjimky nepotřebuje souhlas subjektu údajů, ale takovým zpracováním nesmí pověřit zpracovatele. Z toho však plyne, že snad nejčastější příklad zpracování osobních údajů zpracovatelem uvedený v úvodu této části, tj. outsourcing mzdových agend zaměstnavatele, by vlastně měl být pokládán za odporující zákonu (i když není zcela evidentní, zda to také byl záměr zákonodárce nebo jen omyl v textu zákona).

3.2 Souhlas zaměstnance

Obecně platí, že ke zpracování osobních údajů **potřebuje správce zásadně souhlas** subjektu údajů. Ze souhlasu musí být zřejmé, v jakém rozsahu se poskytuje, tedy jaké osobní údaje smějí být zpracovány. Dále je třeba, aby z něho bylo patrno, kterému správci je dáván souhlas ke zpracování a vymezen jeho konkrétní účel. Souhlas musí zahrnovat také určení období, na které je dáván. Konečně je nutno, aby byl identifikován ten, kdo souhlas poskytuje. Podotkněme, že takový souhlas může dát vždy jen subjekt údajů osobně, a to pouze sám za

sebe. Pokud by subjekt údajů způsobilost k takovému právnímu úkonu neměl, je v tomto smyslu nahrazen určenou osobou (rodičem, opatrovníkem apod.). V žádném případě zde nelze použít analogie režimu společného jmění manželů nebo režimu společného nájmu bytu, byť by šlo takzvaně o vyřizování záležitostí *„obvyklé správy“*, k níž by bylo třeba podobné souhlasy poskytnout a vlastně tak subjekt údajů zavázat trpět omezení svých práv.

Rozsah souhlasu subjektu údajů je omezen přímo zákonem tak, že jím nemohou být dotčeny povinnosti správce či zpracovatele zpracovávat pouze pravdivé a přesné osobní údaje, ověřovat, zda jsou osobní údaje pravdivé a přesné (pokud tak nemůže zjistit, blokovat je), zjistí-li, že údaje nejsou pravdivé a přesné, opět je blokovat a bez zbytečného odkladu opravit nebo doplnit, respektive shromažďovat osobní údaje pouze otevřeně. Tady se z pohledu subjektu údajů jedná o práva, jichž se nemůže vzdát. Tytéž podmínky pak platí i pro souhlas, aby správce mohl zpracovávat osobní údaje k jinému účelu, než k jakému byly shromážděny, respektive i k jinému zpracování osobních údajů, které oprávněně shromáždil bez jeho souhlasu.

Novelou č. 177/2001 Sb. byla ze zákona č. 101/2000 Sb. **vypuštěna povinnost písemné formy** souhlasu (ve stejném režimu by se ovšem nacházela i jeho elektronická forma), z čehož plyne, že by takový souhlas za určitých podmínek mohl být poskytnut i ústně. Zeslabeno bylo i ustanovení, podle nějž není zapotřebí takový souhlas uchovávat po celou dobu zpracování osobních údajů, ale **stačí pouze jeho prokázání**. Z praktických důvodů ovšem ve většině případů bude jistě z hlediska první jistoty nejčastější ona písemná, respektive elektronická podoba. Souhlas může být navíc kdokoliv odvolán, přičemž opět tatáž novela zeslabila toto právo v tom smyslu, že se subjekt údajů může se správcem výslovně dohodnout jinak, tedy zejména na tom, že se práva na odvolání souhlasu předem vzdává. Nicméně právě **povinnost zpracovávat data jen se souhlasem subjektu je v zájmu úměrnosti aplikačním potřebám v různých případech zeslabována**, ovšem vždy se snahou o nalezení optimální úrovně takového zeslabení s maximální možnou ochranou osobních údajů.

Snad nejčastějším příkladem zde bude oprávnění zaměstnavatele zpracovávat osobní údaje bez souhlasu zaměstnance, jestliže provádí **zpracování stanovené zvláštním zákonem nebo nutné pro plnění povinností stanovených zvláštním zákonem**.

Další výjimkou danou praktickými potřebami je možnost zpracovávat údaje bez souhlasu, je-li nezbytné, aby subjekt údajů mohl **vstoupit do jednání o smluvním vztahu nebo aby plnil ujednání smlouvy uzavřené se správcem**.

Pokud je toho nezbytně třeba **k ochraně důležitých zájmů subjektu údajů** (takové zpracování má být zejména v jeho prospěch, ale zpravidla z hlediska jeho časové či prostorové nedostupnosti není prakticky možné souhlas získat v odpovídajícím okamžiku), lze zpracování provést opět bez souhlasu. To však znamená, že posléze je třeba bez zbytečného odkladu takový souhlas získat dodatečně a, pokud by nebyl dán, musí správce zpracování ukončit a údaje zlikvidovat.

Jiná výjimka platí pro osobní údaje, jejichž **zpracování je nezbytné pro ochranu práv zaměstnavatele**. Ta na rozdíl od předchozí může být poměrně častá a z logiky věci celkem průhledná. Zaměstnavatel nemůže být absolutně omezován například ve zpracování osobních údajů, které vypovídají o některých aspektech výkonu práce jeho zaměstnanců a mají tak třeba vliv na jeho prosperitu, jen proto, že s tím zaměstnanec nesouhlasí. Bude sem jistě patřit

široké spektrum možností počínaje zveřejňováním služebních telefonických i jiných kontaktů zaměstnanců nezbytných pro výkon práce, přes sledování telefonních čísel volaných ze služebních telefonů určených pro výkon práce zaměstnance a konče poměrně významnou skutečností, kdy si zaměstnavatel o bývalém zaměstnanci v době po skončení pracovního vztahu ponechá po jistý nezbytný čas k dispozici některé údaje, má-li důvodnou obavu, že by například ještě mohl vzniknout soudní spor o některé nároky či jiná práva z tohoto bývalého vztahu. Podstatné ovšem je, že tuto možnosti má zaměstnavatel, chrání-li práva svá a nikoliv někoho jiného. Takto pak naopak rozhodně není oprávněn běžně sdělovat detailní informace o daném pracovněprávním vztahu veřejnosti, stejně jako třeba soukromou adresu zaměstnance osobě, která tvrdí, že je jeho věřitelem.

3.3 Citlivé údaje

Citlivé údaje patří svým způsobem **do zcela nejintimnější sféry člověka** a v podstatě objektivně (tedy jak z hlediska toho, kdo s nimi hodlá nakládat, tak z hlediska subjektu údajů samotného) je záměrně zkomplikována jejich dostupnost a chování k nim. Dle definice je citlivým údajem takový údaj, který vypovídá *o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů*. Již na první pohled bude zřejmé, že mnohé prvky tohoto seznamu jsou pro pracovněprávní vztahy z věcného hlediska nepodstatné, nepoužitelné a tedy téměř nelze zdůvodnit jejich případné zpracování. Na rozdíl od předchozích období, kdy bývala národnost součástí každého dotazníku či vysvědčení (aniž by však pro čtenáře představovala vůbec nějakou skutečnou zásadní informaci), se výrazně posunul význam tohoto pojmu, a přestože snad z naprosté většiny dotazníků zmizel, nebude v praxi nijak postrádán. Pro využití takových informací jako jsou rasový nebo etnický původ, politické postoje, náboženství, filozofické přesvědčení a otázky sexuálního života subjektu údajů se zřejmě také velmi obtížně bude hledat zdůvodnění, které by nevzbuzovalo podezření alespoň z latentní diskriminace zaměstnance, aktuální či budoucí. V případě zbývajících druhů osobních informací by snad bylo možné některá skutečně objektivní zdůvodnění nalézt.

Zvláštní charakter citlivých údajů se odráží rovněž ve zvláštním přístupu k nim. Především tyto údaje může zaměstnavatel jakkoliv zpracovávat, jestliže k tomu má **výslovný souhlas subjektu údajů**. Souhlas musí být dán bezvýhradně písemně a podepsán subjektem údajů[4]. Ze souhlasu musí být zřejmé, k jakým údajům je dáván, jakému správci údajů, k jakému účelu, na jaké období a kdo jej poskytuje. Na rozdíl od souhlasu v případě obecného zpracování osobních údajů jej může subjekt údajů kdykoliv odvolat a nepřichází zde v úvahu, že by se se zaměstnavatelem dohodl jakkoliv jinak. Tento **souhlas** musí být současně tzv. **kvalifikovaný**, tedy zaměstnavatel je povinen předem subjekt údajů o jeho právech poučit, aby bylo možné usuzovat, že se rozhodl skutečně vážně s plným vědomím všech souvislostí. Takový souhlas musí zaměstnavatel uschovat po dobu zpracování osobních údajů, k jejichž zpracování byl souhlas dán (zpravidla tedy nejméně po dobu trvání pracovněprávního vztahu). Totéž platí obdobně i v případech, kdy zaměstnavatel zpracovával například v nebezpečí z prodlení osobní údaje subjektu údajů v zájmu zachování jeho života a chce případně získat takový souhlas dodatečně.

[4] I zde by měla v situaci běžného zaměstnavatele postačovat například elektronická podoba, za předpokladu, že zaměstnavatel bude s ohledem na okolnosti pořízení takového elektronického souhlasu schopen prokázat autentičnost osoby, která jej dala.

3.4 Informování subjektu údajů

Subjektu údajů se musí dostat **náležité informace o tom, že jsou o něm údaje shromažďovány** již v okamžiku, kdy k této skutečnosti dochází. To zejména proto, aby měl v obecném případě možnost se rozhodnout, jakým způsobem zareaguje ve smyslu ochrany svých práv. Proto je v našem případě zaměstnavatel povinen již před zahájením zpracování osobních údajů povinen subjekt údajů řádně a včas písemně informovat o tom:

- v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány,
- kdo a jakým způsobem bude osobní údaje zpracovávat a
- komu mohou být osobní údaje zpřístupněny či komu jsou určeny.

Opět je zde zmiňována písemná forma, která by v konkrétní situaci mohla být nahrazena některým z jiných způsobů komunikace umožňující trvalý záznam takové informace, než pouze v podobě papírového dokumentu. Novelou byla do tohoto ustanovení zákona přidána možnost, že správce nemusí uvedené informace předat v případě, že jsou subjektu údajů již známy.

Další důležitou povinností zaměstnavatele je **poučit subjekt údajů** o tom:

- zda je podle zákona povinen pro zpracování osobní údaje poskytnout a jaké důsledky budou vyvozeny, pokud tak neučiní,
- kdy je oprávněn odmítnout poskytnutí osobních údajů[5], nebo
- zda poskytnutí osobních údajů je dobrovolné.

Nikoliv již povinně písemnou formou musí zaměstnavatel subjekt údajů informovat o jeho právu přístupu k osobním údajům, zejména tedy o způsobu, jímž se dozví, jaká konkrétní data o něm jsou zpracovávána, respektive obsah těchto údajů.

Častými případy, na něž se vztahuje výjimka z informační povinnosti, jsou:

- zpracování osobních údajů zaměstnavateli **ukládá zákon** nebo je takových údajů třeba k uplatnění jeho práv a povinností vyplývajících ze zvláštních zákonů, nebo
- zpracování osobních údajů **se souhlasem subjektu údajů** (a to jak běžné typy osobních údajů, tak údaje citlivé), respektive
- jedná se o kombinaci obou těchto variant současně,

což bude pravděpodobně splňovat podstatná část veškerých personálních evidencí.

3.5 Oznamovací povinnost

Obecně platí, že osobní údaje lze zpracovávat pouze na základě svolení tzv. orgánu dozoru. Smyslem tohoto ustanovení bylo vytvořit podmínky jak pro efektivní kontrolu zpracování osobních údajů v jeho vlastním průběhu, tak v lepším případě i pro předcházení případných protiprávních zásahů do práv subjektů údajů. Za tímto účelem zákon stanovil povinnost tomu, kdo hodlá zpracovávat osobní údaje (ještě není správcem ve smyslu zákona), takovou skutečnost **oznámit Úřadu pro ochranu osobních údajů**, a to zásadně před zahájením zpracování. Totéž platí i v případě, kdy správce hodlá změnit již dosavadní (třeba i Úřadu oznámené) zpracování osobních údajů v jakémkoliv z podstatných rysů. Oznámení se zásadně podává písemně a musí obsahovat zákonem definované informace.

[5] Toto přichází v úvahu především, pokud by si tím způsobil nebezpečí trestního stíhání.

Úřad je pak povinen do 30 dnů od doručení oznámení oznamovateli sdělit, že jeho **oznámení registruje** (zde se jedná pouze o sdělení této skutečnosti, nikoliv o konstitutivní rozhodnutí podle správního řádu), **nebo** vydat rozhodnutí, kterým **zpracování osobních údajů nepovolí** pro nesplnění podmínek. Pokud Úřad oznámení zaregistroval, může teprve dnem registrace oznamovatel zahájit zpracování osobních údajů. Novelou byly do zákona doplněny mechanismy působící v opačném směru, tj. **možnosti zrušení registrace již zaregistrovaného zpracování osobních údajů** v případě, že správce porušuje podmínky stanovené zákonem. Totéž platí i pro dodatečně doplněnou možnost zrušit registraci v případě zpracování osobních údajů, u nějž pominul účel, pro nějž bylo zaregistrováno.

S ohledem na často problematický charakter a průběh ukončování činnosti správců osobních údajů jako takové (ať již se jedná o podnikatelskou činnost fyzických osob či existenci právnických osob vůbec), je v zákoně pamatováno i na řešení souvisejících problémů. Správce, který hodlá ukončit svou činnost a má u Úřadu registrovaná zpracování osobních údajů, je povinen Úřadu neprodleně **oznámit, jak naložil s osobními údaji** zde zpracovávanými.

3.6 Předávání osobních údajů do zahraničí

Zejména s otevíráním trhu práce roste význam předávání údajů do zahraničí, přičemž se v daném případě může jednat o datovou komunikaci nejrůznějšího typu mezi zaměstnavateli a zaměstnanci, sídly zaměstnavatelských organizací a jejich pobočkami, předávání dat o zaměstnancích veřejnoprávním orgánům jiných států i nejrůznější další způsoby. Zmiňovaný zahraniční prvek není dán pouze například státním občanstvím zaměstnance nebo domicilem zaměstnavatele, ale je sem nutno zahrnout jak zcela fyzické teritoriální umístění materializovaných osobních údajů, tak i jejich dostupnost ze států, kde platí právní normy s příslušnou územní působností (tedy třeba i jejich dostupnost prostřednictvím internetu).

Obecně platí, že z České republiky **do jiných států mohou být osobní údaje předány pouze tehdy, když právní úprava cílového státu, kde mají být zpracovány, odpovídá požadavkům stanoveným v českém zákoně** č. 101/2000 Sb. Prakticky ovšem nepůjde o individuální posuzování dílčích ustanovení jednotlivých zahraničních právních norem, ale v zásadě o kompatibilitu právního prostředí uvedených států, kterou z úřední povinnosti na základě svých institucionálních kontaktů a vazeb posoudí Úřad pro ochranu osobních údajů a výsledek pro jednotlivé státy patřičným způsobem oznamuje. Toto pravidlo je stanoveno ve vztahu ke zcela obecnému adresátovi a tedy se týká jak správců či zpracovatelů osobních údajů, tak subjektů osobních údajů samotných. A zatímco subjekt údajů nelze za nezákonné zacházení se svými údaji účinně postihnout, svědčí uvedené pravidlo zejména správcům osobních údajů.

Tím však není a ani nemůže být řečeno, že se osobní data mohou vždy a všech okolností legálně pohybovat pouze v omezeném prostoru vymezeném příbuzným právem. **Zákon proto stanoví výjimky**, při jejichž nastoupení lze osobní údaje předávat i do těch států, které výše uvedené podmínky nesplňují. Jedná se zejména o specifické situace, kdy:

- předávání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů, který je oprávněn jej učinit,
- je to nezbytné k ochraně práv nebo uplatňování nároků subjektu údajů,
- jde o osobní údaje, které jsou součástí evidencí veřejně přístupných nebo přístupných těm, kdo prokáží právní zájem, avšak jen pokud se týče individuálně určeného údaje nebo údajů,

- předávání vyplývá z mezinárodní smlouvy, jíž je Česká republika vázána,
- předávání je nutné pro uzavření smlouvy mezi subjektem údajů a správcem nebo smlouvy, která je uzavírána v zájmu subjektu údajů, nebo
- je to nezbytné pro záchranu života nebo pro poskytnutí zdravotní péče subjektu údajů,.

Vztáhneme-li uvedené výjimky na případ personálních evidencí apod., vyplývá z tohoto přehledu, že například česká filiálka zahraniční společnosti se sídlem v „nebezpečném státě“ může do své centrály posílat osobní údaje zaměstnanců pouze s jejich souhlasem.

Kromě vyjmenovaných výjimek zaměřených na důvody přeshraničního transportu dat může být předávání osobních údajů uskutečňováno v podstatě z jakéhokoliv důvodu, ovšem provázených ještě tvrdšími předpoklady – musí se tak dít ve prospěch subjektu údajů a mezi správcem a přijímacím subjektem **musí být uzavřena smlouva**, z níž vyplývá, že přijímací strana zajistí požadovanou ochranu osobních údajů.

Před vlastním předáváním osobních údajů do zahraničí je zaměstnavatel povinen požádat Úřad pro ochranu osobních údajů o **povolení k předání nebo předávání osobních údajů do jiných států**.

4. Systematické výjimky

Z předchozího textu zejména vyplynulo, že za určitých podmínek má zaměstnavatel právo si někdy i podstatně zjednodušit vlastní situaci při zpracovávání osobních údajů, a to když s ohledem na jejich vlastnosti, smysl, účel zpracování a obdobné okolnosti může využít některé s výjimek, které mu umožní de facto se vyhnout plnění některých (v klasickém případě nutných obecných) povinností.

Svým způsobem nejpohodlnější je taková situace, kdy zaměstnavatel koná zpracování osobních údajů, které je **upraveno zvláštním zákonem nebo je-li to nutné pro plnění povinností stanovených takovým zákonem**. Pak:
- *nemusí získat souhlas subjektu údajů,*
- *nemusí subjekt údajů informovat ani*
- *nemá registrační povinnost pro takové zpracování osobních údajů*.

Obdobně by se mohl zaměstnavatel zachovat, kdyby hypoteticky zpracovával pouze **oprávněně zveřejněné osobní údaje**.

V případě, že se by se jednalo o zpracování osobních údajů **nezbytné pro oprávněnou činnost politických stran**, politických hnutí, občanských sdružení, odborových organizací, církví nebo náboženských společností, pak by zaměstnavatel:
- *nemusel získat souhlas subjektu údajů,*
- *neměl registrační povinnost pro takové zpracování osobních údajů*
- *a pouze musel subjekt údajů o zpracování údajů nějakou cestou informovat*.

Jednalo-li by se o zpracování osobních údajů určené pro **statistické a vědecké účely**, pak by správce:
- *nemusel získat souhlas subjektu údajů,*
- *nemusel subjekt údajů informovat a*
- *zbyla by mu pouze registrační povinnost pro takové zpracování osobních údajů*.

Mezi takovými kombinacemi důvodů je důležitá i ta situace, kdy zaměstnavatel koná pro **ochranu svých vlastních práv**. V takovém případě by:

- *nemusel získat souhlas subjektu údajů,*
- *musel subjekt údajů o takovém zpracování údajů informovat a*
- *měl také registrační povinnost pro toto zpracování osobních údajů*.

A konečně, pokud se zpracování osobních údajů se děje **se souhlasem subjektu údajů** (případně i výslovným a informovaným):

- *nemá zaměstnavatel povinnost subjekt údajů informovat,*
- *ale tato skutečnost jej nezbavuje registrační povinnosti*.

Výše uvedeného lze ovšem využít vždy pouze tehdy, platí-li takové podmínky na všechny zpracovávané údaje. Jakýkoliv sběr a zpracování údajů byť jen jediného údaje nad rámec rozsahu pokrytého výjimkami již znamená, že výše uvedené povinnosti zaměstnavatel musí splnit (byť by to bylo vůči tomuto jedinému údaji).

Motivy pro takové výjimky a současně pro hledání jejich aplikace v konkrétních situacích však není třeba hledat primárně v nechuti přiznat subjektům údajů jejich obecná nezadatelná práva. Celý systém právních vztahů chránících osobní údaje obsažený uvnitř mnohem širšího spektra nejrůznějších jiných právních vztahů musí být systémově provázaný a logicky kompaktní natolik, aby současně umožnil odpovídající ochranu všem chráněným vztahům a zájmům a zejména pak, aby v se něm nevytvářely neřešitelné kolize. Typickým příkladem by byl stav, kdy by zaměstnavatel byl povinen o zaměstnanci poskytovat státnímu orgánu informace, které by měl právo zpracovávat výhradně se souhlasem zaměstnance, přičemž by daný zaměstnanec předmětný souhlas odmítl dát. Z opačného pohledu lze za kolizní situaci považovat, kdy zaměstnavatel sbírá a zpracovává kvanta informací bez odpovídajícího důvodu s odvoláním na nadneseně široké výklady ustanovení libovolných právních norem, které mu pro daný účel podle jeho názoru patřičné zdůvodnění k reálně protiprávnímu jednání poskytují.

Jako produkt důkladné a podrobné analýzy právních předpisů, které mají jistou vazbu na práva a povinnosti zaměstnavatelů ve vztahu k informacím o jejich zaměstnancích, vznikne několik skupin datových položek, resp. jejich typů, které jsou navzájem příbuzné z hlediska oprávnění k jejich zpracování vůbec a období, po něž takové oprávnění trvá, zvláště.

Do první skupiny patří zejména jméno, příjmení, rodné a všechna další předcházející příjmení a rodné číslo (tj. **základní identifikační údaje**), přičemž tato data je zaměstnavatel oprávněn o zaměstnanci evidovat bez ohledu na jeho souhlas vlastně po celou dobu, kdy o zaměstnanci oprávněně eviduje alespoň jediný další údaj.

Do **druhé skupiny** patří údaje jako jsou datum a místo narození, bydliště, rodinný stav, jména a rodná čísla dětí, manžela a případných dalších osob žijících ve společné domácnosti, jména a další kontaktní údaje rodičů, informaci o případné změněné pracovní schopnosti, informace o relaci vykonávané práce ke zdravotnímu stavu zaměstnance, těhotenství, druhu důchodu, poskytovateli důchodu, datum vzniku nároku na něj, a to vše po takovou dobu, aby i po uplynutí obvyklých uschovacích dob byly zajištěny požadavky vyplývající z jejich použití pro uvedené účely[6]. Rovněž do této kategorie patří veškeré informace, které se v souvislosti s pracovněprávním vztahem zaměstnance k zaměstnavateli vztahují především k evidenci mezd či platů, daní, nemocenskému, důchodovému a sociálnímu pojištění, stejně jako

[6] To plyne z § 31 zákona č. 563/1991 Sb., o účetnictví.

k údajům souvisejícím s bezpečností a ochranou zdraví při práci. Rozhodně sem patří také široce diskutované strhávání členských příspěvků pro odborovou organizaci za situace, kde se ve skutečnosti primárně nejedná o zpracování citlivého osobního údaje o členství zaměstnance v odborech, ale pouze o realizaci srážky ze mzdy.

Do **třetí skupiny** patří údaje jako jsou např. typ státního občanství, identifikace státu a datum změny státního občanství, informace o stupni a oborech vzdělání a datu ukončení, informace o zahájeném trestním řízení pro podezření z úmyslné trestné činnosti spáchané při plnění pracovních úkolů nebo v přímé souvislosti s ním ke škodě na majetku zaměstnavatele, výpis z rejstříku trestů, které je z povahy věci možno evidovat po desetileté promlčecí lhůty od okamžiku ukončení pracovněprávního vztahu[7]. Do téže kategorie současně spadá oprávnění evidovat široké spektrum informací, které v podstatě vznikají v přímé interakci mezi zaměstnancem a zaměstnavatelem a vztahují se ke vzniku, existenci, trvání, průběhu a zániku pracovněprávních vztahů mezi nimi, stejně jako např. informace o konkurenčních doložkách k pracovním poměrům.

Zejména v posledním období je poměrně často diskutovaná na první pohled triviální problematika oprávněnosti evidovat **kontaktní údaje zaměstnance** na jeho pracoviště. Posoudíme-li to se však z pohledu, že kontakt na konkrétní osobu je pro daný účel až sekundární, zatímco primární je zde do jisté míry odosobněná pracovní funkce (na níž je shodou okolností zařazena ona konkrétní osoba) a ta pracovní funkce musí být dovnitř organizace či partnerům a zákazníkům zvenčí dostupná, budou tyto informace výlučně vztaženy na pracovní aktivity, zjevně nebudou vypovídat o soukromém životě zaměstnance a jsou tak vlastně v plné dispozici zaměstnavatele. V tomto smyslu je lhostejné, zda jsou tyto informace užity v interním seznamu, seznamu pro veřejnost, na služebních navštívenkách apod., a to zpravidla pouze po dobu trvání příslušného pracovněprávního vztahu. Zcela jiná situace však platí hned například pro navštívenky zaměstnance, kde by zaměstnavatel hodlal uvádět jeho soukromou adresu, telefon a další údaje. Pak by byl souhlas nezbytný.

Naopak v případě běžného zaměstnavatele v podstatě nelze nalézt právní normu, která by mohla nahradit kvalifikovaný souhlas zaměstnance se **zpracováváním jeho fotografie**. Ovšem je třeba připomenout, že toto platí za předpokladu, že s fotografiemi zaměstnavatel provádí systematické operace. Fotografie v jakékoliv podobě získaná například současně s vyplněním vstupního dotazníku a posléze uložená do spisu dostupného minimálnímu okruhu personalistů není v tomto smyslu osobním údajem právě pro absenci systematického zpracování. A totéž vlastně platí i pro výše zmíněný příklad podnikového průkazu, který je navíc dokonce běžně v držení zaměstnance a nikoliv zaměstnavatele.

Literatura:

1. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, včetně pozdějších novel
2. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech
3. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2000. Praha: ÚOOÚ, 2001
4. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2001. Praha: ÚOOÚ, 2002
5. Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2002. Praha: ÚOOÚ, 2003

[7] Dle § 263 odst. 3 Zákoníku práce.