ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PRÁVNICKÁ

DIPLOMOVÁ PRÁCE

OCHRANA OSOBNÍCH ÚDAJŮ A GDPR

Kateřina Folbrechtová

PLZEŇ 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta právnická
Akademický rok: **2018/2019**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Kateřina FOLBRECHTOVÁ**
Osobní číslo: **R14M0047P**
Studijní program: **M6805 Právo a právní věda**
Studijní obor: **Právo**
Název tématu: **Ochrana osobních údajů a GDPR**
Zadávající katedra: **Katedra pracovního práva a práva sociálního zabezpečení**

Zásady pro vypracování:

1. Úvod do problematiky
2. Práva a povinnosti subjektů při zpracování osobních údajů
3. Úřad pro ochranu osobních údajů
4. GDPR
5. Vnitrostátní právní úprava
6. Současná úprava ochrany osobních údajů v pracovněprávních vztazích
7. Závěr

Rozsah grafických prací:

Rozsah kvalifikační práce:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

- **Listina základních práv a svobod (2/1993 Sb.)**
- **Ústava České republiky (1/1993 Sb.)**
- **Zákoník práce**
- **Zákon o zaměstnanosti**
- **Obecné nařízení o ochraně osobních údajů č. 2016/679 (GDPR)**
- **MORÁVEK, Jakub. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1**
- **NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5**
- **NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7**
- **Zákon o ochraně osobních údajů, komentář C.H. Beck**
- **GDPR/obecné nařízení o ochraně osobních údajů-praktický komentář Wolters Kluwers**
- **https://www.uoou.cz/**

Vedoucí diplomové práce: **Mgr. Miroslav Hromada, Ph.D.**
Katedra pracovního práva a práva sociálního zabezpečení

Datum zadání diplomové práce: **15. února 2018**

Termín odevzdání diplomové práce: **31. března 2019**

Doc. JUDr. Jan Pauly, CSc.
děkan

L.S.

Doc. JUDr. Jarmila Pavlíčková, CSc.
vedoucí katedry

V Plzni dne 13. září 2018

PROHLÁŠENÍ

Prohlašuji, že jsem tuto diplomovou práci na téma „Ochrana osobních údajů a GDPR“ zpracovala samostatně, a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem pro vědeckou práci obvyklým.

V Plzni dne 19. března 2019 …….

Kateřina Folbrechtová

PODĚKOVÁNÍ

Ráda bych tímto poděkovala vedoucímu mé diplomové práce Mgr. Miroslavu Hromadovi, Ph.D. za vstřícnost při jejím vedení, JUDr. et PaedDr. Janě Lindové, PhD. za její ochotu a pomoc a nakonec mé rodině za trpělivost a pevné nervy.

OBSAH

ÚVOD **1**
1. ÚVOD DO PROBLEMATIKY **3**
1.1 Historický vývoj 3
1.2 Vymezení základních pojmů 5
1.2.1 Osobní údaj 5
1.2.2 Citlivý údaj 8
1.2.3 Anonymní údaj 16
1.2.4 Zveřejněný osobní údaj 18
2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ **20**
2.1 Způsoby zpracování osobních údajů 21
2.2 Subjekt údajů 23
2.3 Souhlas se zpracováním osobních údajů 25
2.4 Správce 29
2.5 Zpracovatel 31
2.6 Příjemce 32
2.7 Povinnosti související se zpracováním 33
2.7.1 Stanovení účelu, prostředku a způsobu zpracování § 5 33
2.7.2 Informační povinnost 35
2.7.3 Zabezpečení osobních údajů § 13 39
2.7.4 Oznamovací povinnost 41
3. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ **44**
3.1 Pravomoci a postavení podle GDPR 46
4. GDPR **50**
4.1 Zásady zpracování osobních údajů 52
4.1.1 Zásada zákonnosti 52
4.1.2 Zásada korektnosti a transparentnosti 52
4.1.3 Zásada účelového omezení 52
4.1.4 Zásada minimalizace údajů a zásada přesnosti 53
4.1.5 Zásada omezení uložení 53
4.1.6 Zásada integrity a důvěrnosti 53
4.1.7 Zásada odpovědnosti 53
4.2 Souhlas se zpracováním 54
4.3 Právo na námitku 55

4.4 Právo na přenositelnost osobních údajů 56
4.5 „Právo být zapomenut“ 56
4.6 Posouzení dopadu činnosti na ochranu osobních údajů 57
4.7 Konzultace s Úřadem pro ochranu osobních údajů 58
4.8 Vedení záznamů o zpracovávání osobních údajů 60
4.9 Zabezpečení osobních údajů a hlášení narušení bezpečnosti 61
4.10 Pověřenec pro ochranu osobních údajů 62
5. VNITROSTÁTNÍ PRÁVNÍ ÚPRAVA 70
5.1 Právo na soukromí 70
5.1.1 Soukromí zaměstnance na pracovišti 72
5.2 Občanský zákoník 73
5.3 Zákon o ochraně osobních údajů 74
5.4 Zákoník práce 74
6. SOUČASNÁ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ V PRACOVNĚPRÁVNÍCH VZTAZÍCH 76
6.1 Změny související s přijetím GDPR 77
6.2 Zpracování před vznikem pracovního poměru 80
6.3 Zpracování po dobu trvání pracovního poměru 81
6.3.1 Monitoring zaměstnanců 83
6.4 Osobní údaje zaměstnance po ukončení pracovního poměru 85
ZÁVĚR 86
RESUME 88
SEZNAM ZDROJŮ 89
Bibliografické zdroje 89
Články a internetové zdroje 90
Zákony 91
Judikatura 92
Stanoviska Úřadu pro ochranu osobních údajů a WP29 93

ÚVOD

Ve své diplomové práci jsem se rozhodla zaměřit se na problematiku ochrany osobních údajů. Ochrana osobních údajů je poměrně dynamicky rozvíjejícím se právním odvětvím, ač k jeho významnějšímu rozvoji došlo již v průběhu 20. století. V dnešní době, kterou determinuje především technický pokrok, se jedná o téma velmi diskutované. Důvodem tohoto zájmu se mně osobně jeví především vývoj různých moderních technologií a jejich následné praktické využití, jímž může a často i dochází k zásahu do soukromí subjektů. Toto téma jsem zvolila zejména proto, abych přiblížila aktuální úpravu problematiky ochrany osobních údajů při jejich zpracování, ke kterému dochází každodenně na různých úrovních lidské činnosti. Mnozí ani netuší, co vše do oblasti zpracování osobních údajů spadá. Tato neznalost tak způsobuje jednotlivým subjektům nemožnost využít svá práva.

První komplexní úpravou ochrany osobních údajů byla směrnice 95/46/ES, která byla přijata v rámci EU a její reflexe do českého právního systému proběhla prostřednictvím zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Tato úprava se však vzhledem k rozsáhlému rozvoji výpočetní techniky během posledních let stala již nedostatečnou. Evropská unie se tedy rozhodla na tento technický pokrok reagovat přijetím nařízení, konkrétně se jedná o 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), v praxi běžně označován zkratkou GDPR (General Data Protection Regulation). V práci se tedy zaměřím nejen na úpravu norem dle zákona o ochraně osobních údajů, ale i na tu, jež vyplývá z tohoto nařízení.

Mezi jednu z nejčastějších situací, kdy ke zpracování osobních údajů dochází, je zpracování osobních údajů v intencích pracovněprávního vztahu (mezi zaměstnavatelem a zaměstnancem). Zaměstnavatel zpracovává osobní údaje v rámci zákonné povinnosti, např. v případě vedení evidencí úrazů, ale také z vlastní iniciativy za účelem ochrany svých majetkových práv. Tímto zpracováním tedy dochází ke střetu práva na soukromí a práva na ochranu majetku, přičemž je nutné najít mezi nimi přijatelnou hranici. Také při určování této hranice napomáhá právní úprava i judikatura.

Cílem mé diplomové práce je přiblížit problematiku ochrany osobních údajů běžnému uživateli, definovat základní pojmy a principy, na nichž je tato problematika postavena, seznámit čtenáře se změnami, které s sebou přineslo GDPR a aplikovat ochranu osobních údajů na pracovní právo.

Tuto práci jsem rozdělila na část obecnou a zvláštní a celkově do 6 kapitol. První kapitola bude zaměřena především na historický vývoj celé problematiky a především na vymezení základních pojmů jako je osobní nebo citlivý údaj, bez kterých se v oblasti ochrany osobních údajů nelze orientovat. Kapitola druhá se zaměří na zpracování osobních údajů jako takové včetně vymezení osob, které se na něm podílejí. V kapitole třetí se zaměřím na Úřad pro ochranu osobních údajů, jeho působnost a činnost. Následně v kapitole čtvrté přiblížím poměrně nově přijaté evropské nařízení známé také pod zkratkou GDPR a změny, které s sebou přináší. Poté se budu zaobírat úpravou vnitrostátní, přičemž se budu věnovat také právu na soukromí. Poslední kapitola je zároveň také jedinou kapitolou zvláštní části, v níž se zaměřím na vymezení ochrany osobních údajů v rámci pracovněprávních vztahů, na případy zpracování osobních údajů před uzavřením pracovního poměru, během jeho trvání až po ukončení těchto specifických vztahů.

1. ÚVOD DO PROBLEMATIKY

Osobní údaje a soukromí jako takové, jsou chráněny už po staletí, avšak s rozvojem společnosti a techniky se změnilo nejen to, jak bylo na tyto pojmy nahlíženo, ale i jejich význam pro společnost. Proto také neustále stoupá potřeba tyto informace chránit, a to zejména z důvodu jejich narůstající hodnoty. S rozvojem informačních technologií roste nebezpečí zneužití osobních údajů nejen pro nezákonné účely, kdy příkladem může být krádež identity, prostřednictvím které je následně páchána trestná činnost, nebo zneužití sociálních sítí, které nemají dostatečně zabezpečenu ochranu soukromí, a následné zneužití na nich zveřejněných údajů, popř. špatný výklad těchto zveřejněných faktů, což může zapříčinit kupříkladu ztrátu zaměstnání apod.

Význam osobních údajů je v dnešní době připodobňován obchodním tajemstvím. Aby bylo možné využívat osobní údaje v každodenním obchodním styku, ať už vnitrostátním nebo mezinárodním, je tedy nutné zajistit jejich dostatečnou ochranu a zamezit tak jejich zneužití.

S vývojem chápání důležitosti osobních údajů roste i míra jejich ochrany. Dříve byl kladen význam především na vojenská a státní tajemství, jejichž vyzrazení, popř. zneužití podléhalo nejpřísnějším trestům. Dnes je ochrana vztažena i na údaje soukromých subjektů, na které nebyl dříve brán zřetel. Zvláštní důraz je pak kladen na ochranu tzv. citlivých údajů, mezi které řadíme mimo jiné informace o náboženském vyznání, politické postoje či údaje o sexuální orientaci, kdy i dnes bohužel vyzrazení těchto informací může pro jedince znamenat bezpečnostní riziko.

Ochrana osobních údajů se v současnosti vztahuje pouze na fyzické osoby a je součástí jednoho ze základních práv, tedy práva na ochranu soukromí, které je zaručeno nejen ústavním pořádkem jednotlivých členských států EU, ale i mezinárodními smlouvami a právem Evropského společenství. Právě tato rozsáhlá úprava je důkazem významu, který současná společnost ochraně osobních údajů přisuzuje.

1.1 Historický vývoj

Ochrana soukromí dlouhou dobu vůbec neexistovala a veškeré osobní údaje byly v podstatě veřejné. Jistá ochrana existovala, ale byla nedostatečná

a často odlišná pro jednotlivé společenské vrstvy. Platilo, že čím vyšší vrstva, tím důkladnější ochrana soukromí.

První zlom v ochraně údajů o jednotlivci nastal s příchodem náboženských válek. Příslušnost k odlišnému náboženství se často stávala otázkou boje o přežití, proto si tyto informace lidé začínali více chránit. Dalším zlomem pak byla Velká Francouzská revoluce a Deklarace práv člověka a občana, což byl první psaný text přijatý roku 1789, jenž v určité míře zakotvoval ochranu soukromí. Nejvýznamnější váhu však ochrana osobních údajů získala až v období nacismu. Tehdy se ukázalo, že osobní informace mohou být zneužity také státem. Německý nacistický režim v čele s Adolfem Hitlerem prostřednictvím svých rasových zákonů zapříčinil masovou genocidu lidí s odlišnými názory, náboženstvím a etnikem.

Na Deklaraci z roku 1789 navázala roku 1978 Všeobecná deklarace lidských práv, která se však nikdy nestala závaznou. Nicméně důležitý význam stále má její čl. 12, který říká: *„Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“* Toto bylo později v plném znění přejato do čl. 17 již závazného Mezinárodního paktu o občanských a politických právech.

Prvním komplexním dokumentem, jenž upravoval právo na soukromí, byla až Úmluva o ochraně osobnosti se zřetelem na automatizované zpracování osobních dat, neboli Úmluva č. 108 z roku 1981 a její Dodatkový protokol z roku 2001, který poprvé definoval hlavní zásady ochrany osobních údajů. Tomuto ujednání ještě předcházela Evropská úmluva o lidských právech z roku 1950. Ta však tuto problematiku upravovala jen okrajově v čl. 8, který zakotvoval právo na respektování soukromí a rodinného života.[1]

Vzhledem ke stoupajícímu významu ochrany osobních údajů, roste také legislativní činnost Evropského společenství, které roku 1995 přijalo směrnici 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. Ta zakotvila jednotnou úpravu ochrany osobních údajů a zakázala státům omezit volný pohyb informací mezi členskými zeměmi, čímž umožnila i vznik tzv. Schengenského prostoru. Zmíněná směrnice platila až do května 2018, kdy bylo přijato nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne

[1] Evropská úmluva o ochraně lidských práv.

27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), dnes známé jako GDPR.

1.2 Vymezení základních pojmů

V této kapitole bych ráda definovala základní pojmy důležité pro problematiku ochrany osobních údajů, které se nalézají nejen v ustanoveních zákona na ochranu osobních údajů, ale i v dalších právních předpisech, které se na tuto oblast vztahují. Většina těchto pojmů se nachází v § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, přičemž jejich výklad byl více či méně doslovně přejat ze směrnice 95/46/ES, další jsou pak obsaženy v článku 4 GDPR.

1.2.1 Osobní údaj

Definice pojmu osobní údaj je stěžejní pro celou právní úpravu oblasti ochrany osobních údajů. Aby mohl být údaj označen za osobní, musí splňovat všechny náležitosti jeho definice. Nejsou-li splněny všechny potřebné znaky, pak daný údaj za osobní označit nelze a není tak ani možné použít ustanovení zákona na ochranu osobních údajů. Měla-li by dotčená osoba pocit, že k zásahu do jejího soukromí přesto došlo, musela by se v takovém případě bránit jinými prostředky, konkrétně pak žalobou na ochranu osobnosti, která vychází z občanského práva.

Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat v článku 2 říká, že: *„"Osobní údaje" znamenají každou informaci týkající se identifikované nebo identifikovatelné fyzické osoby („subjekt údajů“).“* Tato definice byla následně plně přejata a rozšířena do článku 2 písm. a) směrnice 95/46/ES. Ten pak říká, že pro účely dané směrnice se rozumí: *„"osobními údaji" 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.“*

Zákon na ochranu osobních údajů zmíněné znění téměř doslovně převzal a doplnil jej o pojem kód a o negativní vymezení, které vymezuje, kdy se o osobní údaj nejedná. Toto ustanovení pak bylo novelizováno pouze

jednou a to tzv. Euronovelou, kde stávající znění paragrafu je tato: *„osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“* Novela tedy reagovala na rozvoj informačních technologií a vypustila tak z definice osobního údaje jeho negativní vymezení, které říkalo, že: *„O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.“* Dnes je totiž možné zjistit identitu fyzické osoby poměrně rychle a bez vynaložení většího úsilí i materiálních prostředků.[2]

Přijetím GDPR následně vznikla další definice osobního údaje, ta je však obsahově téměř shodná s definicí v zákoně o ochraně osobních údajů. Toto nařízení pak termín „osobní údaj“ ve svém článku 4 odstavci 1 vykládá 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.“*

Pro definici osobního údaje je důležité především to, že jím může být jen informace týkající se subjektu údajů, tím je pouze fyzická osoba. Zákon na ochranu osobních údajů se totiž právnických osob netýká. Aby se jednalo o osobní údaj, musí se daná informace týkat určeného či určitelného subjektu údajů, resp. identifikované nebo identifikovatelné fyzické osoby. O osobní údaj se tedy jedná tehdy, je-li osoba, která informací disponuje, schopna ji přiřadit ke konkrétnímu člověku, popř. pomocí ní konkrétního člověka určit.

Rozhodujícím pak je to, kdo s danou informací disponuje. Zatímco jeden správce určí na základě stejné informace konkrétní osobu naprosto bez problémů, pro jiného může být tato informace nepoužitelná, tedy nedůležitá. Zde bych se ráda zmínila o tzv. šifrovaných informacích a pseudonymizovaných údajích. K jejich chápání a interpretaci je potřeba znát klíč, z čehož vyplývá, že ten, kdo disponuje takovým údajem, ale nemá klíč, nebude moci šifrovaný údaj použít

[2] Důvodová zpráva k zákonu č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů: k bodu 7 – změna § 4 písm. a).

ani využít k další identifikaci, protože bez znalosti klíče takový údaj pozbývá jakékoli výpovědní hodnoty. Jedná se kupříkladu o zákaznické číslo. Šifrovaná informace není bez znalosti klíče osobním údajem, což vyplývá také z judikatury NSS.

Například v rozsudku sp. zn. 1 As 98/2008 ze dne 29. července 2009 NSS konstatoval, že za osobní údaj není považováno jméno a příjmení fyzické osoby v kombinaci s číslem občanského průkazu ve smyslu § 4 písm. a) zákona o ochraně osobních údajů, nýbrž ani na základě těchto údajů není možné konkrétní osobu určit nebo kontaktovat. Neexistuje totiž žádný veřejně dostupný registr čísel občanských průkazů, v němž by bylo možné zjistit identitu osoby podle čísla občanského průkazu. Navíc v případě čísla občanského průkazu se jedná o označení, které je v průběhu času proměnlivé. Fyzická osoba totiž neobdrží jedno číslo občanského průkazu na celý život, nýbrž při každé výměně tohoto průkazu získává průkaz s číslem novým. Ani ve spojení tohoto čísla se jménem a příjmením fyzické osoby nelze zpravidla zjistit konkrétní identitu.

Určitelným pak bude také ten subjekt, pro jehož určení bude správce muset vyvinout větší snahu, která bude spočívat zejména v zjištění více informací, nejčastěji z veřejně dostupných databází, které mu pak spolu s původní informací pomohou dosáhnout jeho cíle, neboli určení konkrétní osoby. Subjekt údajů se považuje za učený, jestliže správce disponuje jeho přímými identifikačními údaji, podle nichž má možnost zjistit jeho identitu a dohledat jej. Tato identifikace by byla považována za identifikaci nepřímou. Naopak v případě, že bychom byli schopni určit danou osobu podle údaje, jímž disponujeme, jednalo by se o identifikaci přímou.[3]

Osobním údajem může být jakákoliv informace, která nám o konkrétní osobě něco vypoví. Tyto informace pak můžeme dělit na údaje identifikační, adresní a popisné.[4] Pomocí identifikačních údajů určujeme osobu přímo, jedná se o jméno, příjmení, údaje číselné hodnoty, jako je například datum narození, a v neposlední řadě místní názvy. Údaje adresní slouží také k identifikaci určité osoby, avšak je zde odlišný způsob, jakým lze identifikace dosáhnout a konkrétní osobu tak najít. Patří sem adresa trvalého pobytu, doručovací adresa, telefonní číslo apod. Poslední kategorií jsou údaje popisné. Jedná se o všechny údaje,

[3] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 16.
[4] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5, s. 53–76.

které nám určitou osobu popisují a vytvářejí tak komplexní obraz fyzické osoby. Ať už je to vzhled, věk a výška nebo vlastnosti osoby popř. její zájmy, vzdělání či zaměstnání.

Pojem osobní údaj je definován i v jiných právních předpisech, jako je například zákon o svobodném přístupu k informacím, trestní zákoník nebo třeba zákoník práce. Avšak pro určení, zda je informace osobním údajem či nikoli, je vždy nutné použít definici obsaženou v zákoně o ochraně osobních údajů.

1.2.2 Citlivý údaj

Citlivý údaj je zvláštním typem osobního údaje, který obsahuje kromě běžných informací o fyzické osobě také informace zvláštního charakteru, čímž dochází k intenzivnějšímu zásahu do soukromí jedince. Je zde proto kladen větší důraz na jejich ochranu a jsou také stanoveny přísnější podmínky pro jejich zpracování. Pojem „citlivý údaj“ však zná jen český zákonodárce, v mezinárodním styku se používá označení zvláštní kategorie údajů, což můžeme vidět v Úmluvě č. 108 i ve směrnici 95/46/ES.

Aby mohl být údaj označen za citlivý, musí splňovat náležitosti § 4 písm. b) zákona o ochraně osobních údajů. Za citlivý údaj je tedy považován *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů, citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci osob nebo autentizaci subjektu údajů.“* Tato definice prošla několika novelizacemi – konkrétně novelami č. 177/2001 Sb., č. 439/2004 Sb. a č. 170/2007 Sb., kde oproti původnímu znění zákona výraz „o politických postojích“ nahradil termín „členství v politických stranách a hnutích“ a stejně tak pojem „členství v odborových organizacích“ nahradil slovní obrat „o členství v zaměstnaneckých organizacích“. Významnou je pak změna, která nastala přijetím zákona č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru, kde došlo ke změně v oblasti biometrických údajů a jejich aplikace. Nově je zde upřesněno, že se jedná o biometrická data, jejichž prostřednictvím lze subjekt údajů přímo identifikovat či autentizovat.[5]

[5] Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.

Definici zvláštní kategorie údajů najdeme také ve směrnici 95/46/ES v čl. 8 odst. 1, který takovýto údaj označuje za „*osobní údaj, který odhaluje rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i údaj týkající se zdraví a sexuálního života*.“ Porovnáme-li obě ustanovení, dojdeme k závěru, že definice jsou téměř totožné, pouze ve směrnici chybí údaj o trestné činnosti subjektu, kterému však směrnice ve svém ustanovení článku 8 odst. 5 vymezuje zvláštní režim.

Termínu zvláštní kategorie údajů pak využívá i Úmluva č. 108 ve svém článku 6, který říká, že „*osobní údaje prozrazující rasový původ, politické názory, náboženské nebo jiné přesvědčení, jakož i osobní údaje týkající se zdraví nebo pohlavního života smějí být zpracovány automatizovaně jen tehdy, jestliže vnitrostátní právní řád stanoví vhodné záruky. Stejně tomu je u osobních údajů týkajících se odsouzení za trestný čin.*“

Na zpracování citlivých údajů jsou kladeny daleko větší nároky než na zpracování údajů osobních, a to zejména proto, že při jejich nesprávném zpracování nebo zneužití by došlo k mnohem většímu zásahu do soukromí, než ke kterému může dojít u osobních údajů. Problematika zpracování citlivých údajů je upravena v § 9 zákona o ochraně osobních údajů. Tyto údaje mohou být zpracovávány jen v takovém případě, kdy správce, resp. zpracovatel citlivých údajů obdržel od subjektu údajů kvalifikovaný souhlas s jejich zpracováním. Subjekt musí být před udělením souhlasu informován ve smyslu § 12 a § 21 o tom, pro jaký účel budou informace zpracovávány, jaké údaje budou zpracovávány, kdo je bude zpracovávat a po jakou dobu. Tato informační povinnost je stejná jako u zpracování osobních údajů, kterou se budu zabývat posléze. Správce také musí být existenci souhlasu subjektu schopen prokázat po celou dobu zpracování citlivých údajů. Zpracování citlivých údajů bez souhlasu subjektu údajů je možné jen za zákonem předvídaných právních situací, které jsou taxativně vymezeny právě ustanovením § 9 zákona o ochraně osobních údajů, toto ustanovení nelze rozšiřovat. Vzhledem k obsáhlosti tohoto paragrafu se zaměřím jen na některé z nich.

Souhlas subjektu údajů není nutný v případě, kdy je zpracování nutné v zájmu zachování života a zdraví subjektu údajů nebo jiné osoby, pro odvrácení bezprostředního nebezpečí hrozícího jeho majetku nebo pokud není jeho souhlas možno získat zejména z důvodu fyzické, duševní či právní nezpůsobilosti, většinou v případě, kdy je nezvěstný nebo za jiných obdobných okolností.

Správce je však v tomto bodě povinen ukončit zpracování a zlikvidovat shromážděné údaje ihned, pominou-li uvedené okolnosti, ledaže by správce ke zpracování obdržel souhlas subjektu dodatečně. V tomto případě se tedy bude vždy jednat o zpracování dočasné a krátkodobé. Tato výjimečná situace se bude v praxi vyskytovat jen výjimečně, protože je možné ji použít jen v krizových až extrémních situacích.

Dále mohou být citlivé údaje zpracovávány pro účely poskytování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění a pro výkon státní správy v oblasti zdravotnictví. Do této kategorie spadá také posuzování zdravotního stavu. Ve všech stanovených případech je také daná problematika upravena zvláštním zákonem. Typickým příkladem této kategorie je vedení zdravotnické dokumentace a nakládání s ní zdravotnickými zařízeními. Pro všechny pracovníky, kteří zpracovávají, popř. přicházejí do styku s citlivými údaji podle § 9 písm. c) platí shodně povinnost zachovávat mlčenlivost v souladu s ustanoveními § 15 zákona o ochraně osobních údajů a ustanoveními zvláštních zákonů, které danou oblast upravují.

Citlivé údaje lze zpracovávat i tehdy, je-li to nutné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovněprávních vztahů, což je stanoveno zvláštním zákonem. Nejčastěji půjde o zpracování podle zákoníku práce. Může jít například o zpracování zdravotních údajů v souvislosti s pracovním úrazem zaměstnance nebo s nemocí z povolání. Zaměstnavatel je taktéž povinen vést knihu úrazů podle ustanovení § 105 zákoníku práce a vést evidenci zaměstnanců, u nichž se projevila nemoc z povolání, dále pak musí zpracovávat zdravotní údaje těhotných zaměstnankyň, které u něj chtějí uplatňovat svá práva dle ustanovení § 239 až § 241 zákoníku práce, jako například právo na převedení na jinou práci, převod z noční na denní práci nebo zákaz přesčasů aj. Další případy, kdy lze citlivé údaje zpracovávat bez souhlasu subjektu údajů nalezneme v ustanovení § 9 zákona o ochraně osobních údajů.

Nyní bych se ráda zaměřila na přesnější vymezení kategorií citlivých údajů, a to především z důvodu, že při jejich výkladu může dojít k jisté subjektivizaci. Velmi často se objevují snahy význam těchto kategorií zúžit či rozšířit s ohledem na to, kdo a jaké údaje zpracovává. Význam jednotlivých kategorií nelze zúžit, protože by tak mohlo dojít k nedodržení pravidel pro zvýšenou ochranu citlivých údajů, které jsou zaručeny právem vnitrostátním, mezinárodním i evropským. Také však nelze pojmy rozšířit, neboť by sem mohla

být zařazena i data, jejichž zpracovávání ze své podstaty do soukromí nepřiměřeně nezasahuje.[6]

Informace o původu člověka

Do této skupiny citlivých údajů můžeme zařadit informace o národnostním, rasovém či etnickém původu člověka. Tato kategorie je zaměřena na vrozené charakteristiky člověka, které jsou až na národnost, kterou si může v českém právu každý svobodně zvolit, v zásadě neměnné.[7]

Je důležité zmínit, že národnost a státní příslušnost nejsou pojmy totožné. Zatímco zaměstnavatel může zpracovávat informace o státním občanství, o národnosti toto nelze. Národnost je chápána jako příslušnost k určitému národu, národnostní nebo etnické menšině, oproti tomu občanství je chápáno jako místně neomezený právní svazek státu a fyzické osoby.

Problém nastává v případě kamerových záznamů a fotografií, ze kterých je rasový či etnický původ zachyceného člověka patrný. Slouží-li tedy kamery k monitorování určitého prostoru za účelem prevence protiprávního jednání, nejčastěji poškození majetku správce, je účelem zpracování identifikace konkrétní osoby, která se protiprávního skutku dopustila. Primárně jsou tedy zpracovávány údaje identifikační. Přestože tedy záznam může určité citlivé informace obsahovat, nebude se jednat o jejich zpracování, protože k jejich shromáždění došlo nahodile a nebylo cílem pořízení záznamu. V případě posouzení tohoto případu je tedy klíčový účel zpracování, který nesmí být naplněn pomocí citlivých údajů. Ke shromáždění citlivých údajů tedy nesmí dojít účelně, nýbrž náhodně.[8] O zpracování citlivých údajů by se však jednalo v případě, že by byl kamerový systém vybaven softwarem pro vyhodnocení a následné přiřazení získaných biometrických informací k informacím běžně zpracovávaným.

Informace o názorech a přesvědčeních člověka

Další důležitou kategorií jsou informace týkající se názorů a přesvědčení člověka, kam spadají politické postoje, členství v odborových organizacích nebo náboženské a filozofické přesvědčení. Cílem je zařadit do této kategorie veškeré životní postoje a názory nehledě na to, jakým způsobem jsou učiněny. Spadají

[6] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 55.
[7] Tamtéž, s. 56.
[8] Tamtéž, s. 56.

sem tedy údaje vyplývající jak z písemných, tak ústních záznamů, ze kterých lze určit informace o politických nebo náboženských postojích.

Ráda bych také uvedla, že pojem politický postoj je pojmem širším oproti výrazu členství v politické straně. Lze sem zařadit i informace o hlasování ve volbách nebo záznamy o účasti na politických demonstracích. Hranice této kategorie je však dosti nejasná. V souvislosti s tím lze zmínit např. Ústavního soudu ČR sp. zn. I. ÚS 517/10 ze dne 15. listopadu 2010, kde soud konstatoval, že členství v politické straně samo o sobě (v tomto případě členství v totalitní KSČ), není dle ústavně konformního výkladu údajem o politických postojích subjektu údajů ve smyslu § 4 písm. b) zákona o ochraně osobních údajů, a tudíž se nejedná o citlivý údaj, k jehož zpracování by bylo třeba souhlasu subjektu údajů. Jedná se tedy pouze o údaj osobní ve smyslu § 4 písm. a) zákona o ochraně osobních údajů. Členství v KSČ totiž nebylo podmíněno sdílením jejích názorů, někteří do strany vstoupili, přestože myšlenky a cíle KSČ nesdíleli a chtěli jen požívat výhod členství. Nutno však vzít v úvahu rozdíl mezi totalitní a jinou politickou stranou. Dnes totiž členství v politické straně o názorech, minimálně o příslušnosti k okruhu určitých politických postojů, většinou vypovídá, z čehož by pak vyplývalo, že se o údaj citlivý jedná. Lze si sice představit, že by členství i v dnešní době o politických postojích nevypovídalo, v takovém případě by však bylo nutné zdůvodnit, proč tomu tak není.

Specifickou kategorií je pak členství v odborové organizaci, které vypovídá minimálně o vůli zaměstnance se aktivně podílet na prosazování jeho práv. Tato informace by však mohla být pro zaměstnavatele zásadní. Zájmy zaměstnavatele jsou totiž většinou v rozporu se zájmy nebo požadavky odborových organizací a údaj o členství zaměstnance v takovéto organizaci by mohl způsobit jeho následnou diskriminaci ze strany zaměstnavatele, proto jsou tyto údaje považovány za citlivé a spadají tak pod přísnější právní režim. S členstvím v odborových organizacích souvisí také placení příspěvků prostřednictvím zaměstnavatele, nejčastěji formou srážky ze mzdy nebo platu, v takovém případě by mělo být s takovými údaji taktéž zacházeno jako s údaji citlivými.[9]

Pojem filozofické přesvědčení byl zahrnut do kategorie citlivých údajů hlavně proto, aby nedocházelo ke spekulacím o tom, zda do citlivých údajů patří

[9] MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5, s. 81.

jen informace o příslušnosti ke státem uznané církvi nebo i údaje o příslušnosti k neregistrovaným náboženským společnostem.[10] Dle zákona o ochraně osobních údajů a LZPS musí požívat stejné právní ochrany údaje o náboženství i jakékoli záznamy o filozofických názorech osoby.

Informace o osobním životě

Do této kategorie lze zařadit údaje o odsouzení za trestný čin a údaje o zdravotním stavu a sexuálním životu subjektu.

Nejdříve se zaměřím na údaje o odsouzení za trestný čin. Jak již z názvu kategorie plyne, nelze sem zařadit informaci o tom, že někdo určitý trestný čin nespáchal popř. informace o jednání subjektu, které by však nenaplňovalo znaky trestného činu. Nespadají zde tedy informace o přestupku, o podmíněném zastavení trestního stíhání dle § 307 zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen jako „trestní řád“) ani o narovnání podle § 309 trestního řádu, neboť se o informace o odsouzení za trestný čin nejedná. Zaměstnavatel může požadovat výpis z rejstříku trestů jen tehdy, vyžaduje-li to charakter vykonávané práce, tento údaj pak bývá často zakládán do osobních spisů zaměstnanců. Pro zaměstnavatele je však vhodnější si údaj o trestní bezúhonnosti zaměstnance pouze vyznačit a neuchovávat tak celý výpis z evidence.

Až do přijetí euronovely byl tento pojem chápán poněkud obsáhleji. Uvedenou novelou došlo k zúžení tohoto výkladu, pojem „údaj vypovídající o trestné činnosti osoby“ byl nahrazen „údajem o odsouzení za trestný čin“.[11] Podle všeobecného názoru se tedy za citlivý údaj bude považovat pouze informace o existujícím odsouzení za trestný čin, která by byla obsažena ve výpisu z rejstříku trestů. Opačná situace však může nastat v případě opisu z rejstříku trestů, ten totiž obsahuje informace o každém odsouzení fyzické osoby, a to i o těch zahlazených.[12]

Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů je také nově upraveno ve článku 10 nařízení Evropského parlamentu a Rady (EU) 2016/679, který říká, že zpracování těchto údajů podléhá dozoru orgánu veřejné moci. Není-li tedy tento dozor vykonáván, nelze tyto údaje zpracovávat. Ke zpracování těchto údajů by ještě mohlo dojít v případě,

[10] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 58.
[11] Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
[12] Zákon č. 269/1994 Sb., o Rejstříku trestů.

kdy by bylo zpracování oprávněné podle práva Unie nebo členského státu poskytujícího dostatečné záruky, šlo-li by o práva a svobody subjektu údajů. Jakákoli evidence rejstříku trestů může být vedena výhradně jen pod dozorem orgánů veřejné moci.

Dále lze do kategorie informací o osobním životě považovaných za citlivé údaje zařadit všechny informace týkající se fyzického či psychického zdraví subjektu údajů, včetně informace o schopnosti vykonávat určitou činnost, údaje o vyšetření, hospitalizaci, závislosti nebo užívání návykových látek a také informace o těhotenství. Podle GDPR by pak byly za údaj o zdravotním stavu považovány všechny osobní údaje, které by se týkaly tělesného nebo duševního zdraví fyzické osoby včetně údajů o poskytnutí zdravotních služeb, které by vypovídaly o jejím zdravotním stavu.[13]

Informacemi vypovídajícími o sexuálním životě subjektu jsou myšleny především údaje o sexuální orientaci subjektu a údaje o provozovaných sexuálních praktikách, popř. informace o sexuálním partnerovi.[14]

Genetický a biometrický údaj

Nejvíce se rozvíjející kategorií oblasti zpracování citlivých údajů je zpracování genetických a biometrických údajů, která částečně souvisí s údaji o zdravotním stavu subjektu.

Za genetické údaje jsou považovány informace získané rozborem lidské deoxyribonukleové kyseliny (DNA), údaje z tohoto procesu zjištěné vypovídají nejen o zdravotních a dědičných dispozicích jedince, ale také o třetích stranách neboli předcích a potomcích této osoby. Podle článku 4 odst. 13 GDPR jsou genetickými údaji: „*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*.“ Vzhledem k rozvoji medicíny, vědy a techniky je ochrana těchto údajů velmi důležitá z důvodu přístupnosti metod pro rozbor DNA, ale i z důvodu jejich komerčního využití.

Nejvýznamnější oblastí, kde se rozbor DNA využívá, jsou mezinárodní databáze DNA. K jejich rozvíjení a rozšiřování dochází prakticky neustále.

[13] Čl. 4 odst. 15 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[14] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 59.

Nejvíce jsou pak tyto databáze využívány orgány činnými v trestním řízení, kdy jsou nejčastěji zpracovávány kriminalistickým ústavem zejména k identifikaci osob či nalezených tělesných ostatků, případně mohou sloužit jako důkaz výskytu osoby na konkrétním zkoumaném místě. Vzhledem k přesnosti metody rozboru DNA je její přínos pro policejní účely zjevný. Přístupem k národní databázi DNA disponuje i Policie ČR, která ji v rámci své činnosti doplňuje o genetický materiál osob podezřelých ze spáchání trestného činu, osob odsouzených pro spáchání úmyslného trestného činu, osob pohřešovaných apod.[15] V databázi jsou také uchovávány profily nálezů lidských ostatků a vzorky, které byly nalezeny na místech činu, avšak nikdy nedošlo k jejich identifikaci a tím pádem ani k vyřešení daných případů. Rostoucí obsah databáze tedy dává naději tomu, že k objasnění nevyřešených případů možná jednou v budoucnu dojde.

Až do okamžiku přijetí nařízení Evropského parlamentu a Rady (EU) 2016/679 nebyla definice biometrického údaje a jeho případná ochrana v českém právním řádu vůbec obsažena a nenašli bychom ji ani v mezinárodních či evropských pramenech. Bylo tedy nutno vycházet z jeho obecného významu, tj. že biometrický údaj je měřitelný fyzický či fyziologický a po dobu života člověka prakticky neměnný znak, který umožňuje zjištění nebo ověření identity dané osoby. Biometrika slouží k jednoznačné identifikaci osob na základě jedinečných a měřitelných znaků člověka, jakými jsou otisky prstů, chodidel či dlaní, obraz oční sítnice nebo duhovky, záznam dynamického projevu chůze a rozbor tváře či hlasového projevu. Podle již zmíněného GDPR, konkrétně pak článku 4 odst. 14 jsou biometrickými údaji: *„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 rozpoznání obličeje nebo daktyloskopické údaje.“* Dnes se s využitím biometrických údajů setkáme zejména při kontaktu s orgány veřejné správy, jsou obsaženy například v cestovních dokladech apod. Vzhledem k rozvoji této oblasti jsou také stále více využívány i v soukromém sektoru, především pak jako bezpečnostní opatření pro vstup do zabezpečených objektů, tj. jako docházkové systémy, ale také jako odemykací prvek pro přístup do mobilních zařízení.

S přijetím tzv. schengenské novely došlo k modifikaci definice citlivého údaje v zákoně o ochraně osobních údajů, kdy je jeho aplikace ve vztahu

[15] § 35 odst. 1. zákona č. 273/2008 Sb., o Policii České republiky.

k biometrickým údajům omezena pouze na taková biometrická data, jejichž prostřednictvím lze subjekt přímo identifikovat, tedy zjistit totožnost dané osoby, nebo autentizovat, čili ověřit proklamovanou identitu dané osoby.[16] Došlo tak k celkovému zúžení významu tohoto termínu, kdy je zvýšená ochrana vymezena jen pro ty údaje, které mohou přímo sloužit k identifikaci či odlišení osob.

Ráda bych zde zmínila problematiku povahy rodného čísla. To je sice mnohými považováno za údaj citlivý, avšak opak je pravdou. Citlivými jsou pouze ty údaje, které jsou stanoveny v taxativním výčtu ustanovení § 4 písm. b) zákona o ochraně osobních údajů, a toto ustanovení nelze dále rozšiřovat. Rodné číslo je tedy pouze údajem osobním, a tak jeho zpracovávání nepodléhá zvláštnímu režimu určenému pro zpracování citlivých údajů. Nicméně práci s rodnými čísly existuje vlastní úprava, a to v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, kde je mimo jiné upraven i postup, jak je možné s rodnými čísly nakládat a kdy je lze využívat.

1.2.3 Anonymní údaj

Za anonymní údaj je dle § 4 písm. c) zákona o ochraně osobních údajů považován takový údaj, který: „*buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů*.“ Je to tedy každý takový údaj, jehož prostřednictvím není subjekt údajů identifikovaný ani identifikovatelný, a to ani správcem ani jakoukoli jinou třetí stranou. Takový údaj neobsahuje žádnou charakteristiku či jedinečný znak dotyčné osoby.[17] Jsou to tedy údaje zbavené jména, příjmení a rodného čísla, které je tak možné využívat např. pro vědecké nebo statistické účely. V případě, že by bylo možné pomocí tohoto údaje fyzickou osobu jakkoliv identifikovat, nejednalo by se již o údaj anonymní. Za anonymní tedy nejsou považovány údaje, u nichž správce od osobních údajů identifikační údaje pouze odpojil, avšak kterými on nebo kdokoliv jiný i nadále disponuje, byť jsou v oddělené formě, protože zde stále existuje možnost jejich opětovného propojení. V takovém případě by se jednalo o údaje pseudonymní, ty jsou mimo jiné využívány v případech zveřejňování judikatury Nejvyšších soudů.

Na základě výše uvedeného lze tedy rozlišit dvě skupiny anonymních údajů. Údaje částečně anonymní, resp. pseudonymní, kdy subjekty nejsou pro

[16] Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru.
[17] Důvodová zpráva k zákonu č. 101/2000 Sb., o ochraně osobních údajů ze dne 22. 9. 1999.

toho, kdo momentálně informaci drží, identifikovatelné, avšak v případě opětovného propojení informací by možnost identifikace subjektu opětovně vznikla, a údaje plně anonymní, kdy nemožnost identifikace subjektu se nebude omezovat jen na čas přítomný, ale i na čas budoucí. Údaje pseudonymní zákon o ochraně osobních údajů za anonymní údaje ve smyslu § 4 písm. c) nepovažuje, jsou však používány v mnoha sférách, ať už jako zákaznická čísla, forma zabezpečení osobních údajů, v oblasti vzdělávání v případě přijímacích zkoušek atd. Pseudonymních údajů je také využíváno při zveřejňování informací o obětech trestné činnosti, což je umožněno ustanovením § 8a[18] a § 8b[19] trestního řádu.

Anonymními mohou být údaje od počátku nebo se jimi mohou teprve stát, a to po provedení tzv. anonymizace. Anonymizovaný údaj je takový údaj, který byl původně vztažitelný k určitému subjektu, avšak po provedení anonymizace toto provést již nelze. Jak již bylo zmíněno, anonymizované údaje se mohou používat pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. *„Správce je povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování, ale pro výše zmíněné účely mohou být osobní údaje uchovány i po uplynutí této doby. Nicméně je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a proto se osobní údaje mají anonymizovat, jakmile to bude možné.“* [20]

Na anonymní, resp. anonymizované údaje se tedy nevztahují zásady ochrany osobních dat, což je stanoveno v článku 26 směrnice 95/46/ES, který říká, že: *„zásady ochrany se nevztahují na údaje, které byly učiněny anonymními tak, že dotčená osoba již není identifikovatelná“*, ani ustanovení zákona o ochraně osobních údajů, poněvadž anonymní údaje nejsou údaji osobními.

Nově přijaté nařízení 2016/679 v článku 4 odst. 5 definuje pouze proces „pseudonymizace“. Za ten se pak považuje takové zpracování osobních údajů, které znemožňuje jejich opětovné přiřazení ke konkrétnímu subjektu údajů bez použití dodatečných informací. Tyto informace jsou pak uchovávány odděleně

[18] § 8a odst. 1 věta druhá zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád): „*V přípravném řízení nesmějí při poskytování informací o své činnosti veřejnosti orgány činné v trestním řízení zveřejnit informace umožňující zjištění totožnosti osoby, proti které se vede trestní řízení, poškozeného, zúčastněné osoby a svědka.*“

[19] § 8b odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád): „*Nikdo nesmí v souvislosti s trestným činem spáchaným na poškozeném jakýmkoli způsobem zveřejnit informace umožňující zjištění totožnosti poškozeného, který je osobou mladší 18 let nebo vůči němuž byl spáchán trestný čin …*“

§ 8b odst. 4: „*Pravomocný rozsudek nesmí být zveřejněn ve veřejných sdělovacích prostředcích s uvedením jména, popřípadě jmen, příjmení a bydliště poškozeného uvedeného v odstavci 2*.“

[20] § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

a vztahují se na ně technická a organizační opatření, aby nemohlo dojít k tomu, že budou znovu přiřazeny k identifikované či identifikovatelné fyzické osobě. S tímto vymezením souvisí i znění článku 11 téhož nařízení, které vymezuje zpracování, k němuž není třeba identifikace. Je zde stanoveno, že pokud účely, pro něž správce informace zpracovává, již nevyžadují identifikaci subjektu údajů, nemá správce povinnost tyto údaje, jež by sloužily k jeho identifikaci, dále uchovávat, získávat nebo zpracovávat. Je-li pak schopen správce doložit, že není ve zmíněných případech schopen subjekt údajů identifikovat, informuje o tom subjekt údajů, je-li to možné. V takovém případě by se neužila ustanovení článků 15 až 20 daného nařízení, která se týkají práva subjektu na přístup k osobním údajům, práva na opravu a výmaz, práva na omezení zpracování, oznamovací povinnosti v případě opravy či výmazu a práva na přenositelnost údajů, s výjimkou případů, kdy by subjekt, za účelem výkonu svých práv, doložil dodatečné informace potřebné k jeho následné identifikaci.[21]

1.2.4 Zveřejněný osobní údaj

Zveřejněným osobním údajem je podle ustanovení § 4 písm. a) zákona o ochraně osobních údajů „*osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu*“. Zveřejnění je nutno chápat jako systematickou činnost správce osobních údajů ve smyslu ustanovení § 4 písm. e) zákona o ochraně osobních údajů.

Vzhledem k tomu, že zákonodárce v definici použil pojem zpřístupnění, který je, spolu se zveřejněním, formou zpracování osobních údajů, je třeba si tyto pojmy odlišit. Domnívám se, že zveřejnění bude spočívat v „podání“ osobního údaje neurčitému počtu adresátů pomocí hromadných sdělovacích prostředků, jimiž jsou periodický tisk, rozhlas a televize. Myslím si, že mezi hromadné sdělovací prostředky lze začlenit i internet, jakožto moderní formu sdělovacího prostředku. Oproti tomu zpřístupnění lze dle mého názoru chápat ve smyslu zpřístupnění osobního údaje užšímu, popř. přesně vymezenému počtu adresátů.

[21] Čl. 4, 11 a 15 až 20 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Na rozdíl od aktu zveřejnění se v tomto případě nebude jednat o tzv. širokou veřejnost i přesto, že okruh adresátů se může zdát poměrně rozsáhlý.[22]

V případě, kdy by mělo dojít ke zpracování oprávněně zveřejněných osobních údajů, pak není zapotřebí souhlasu subjektu údajů. Za řádně zveřejněné lze považovat údaje obsaženy ve veřejných seznamech, které jsou součástí zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob. Jsou jimi kupříkladu katastr nemovitostí, obchodní rejstřík nebo živnostenský rejstřík. Na tyto údaje se zároveň nevztahuje poučovací[23] ani oznamovací[24] povinnost. I těmto údajům je však poskytnuta určitá ochrana nalézající se v ustanovení § 5 odst. 2 písm. d) zákona o ochraně osobních údajů.

K problematice zpracování se taktéž vyjádřil Úřad pro ochranu osobních údajů ve svém stanovisku.[25] Konstatoval zde, že e-mailová adresa obsahující jméno a příjmení zaměstnance je sama o sobě osobním údajem. Jestliže tedy nejsou zaměstnanci zástupci firmy navenek, bude ke zveřejnění jejich e-mailové adresy nutné získat jejich souhlas, bez něhož by se jednalo o zveřejnění neoprávněné. Tento postup je aplikovatelný i na další údaje zaměstnance, např. jméno a příjmení, fotografie a kontakt, které by chtěl zaměstnavatel uveřejnit kupříkladu na svých internetových stránkách.

[22] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 18–19.
[23] § 11 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[24] § 16 a § 18 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[25] K problémům z praxe – č. 1/2003 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců. *Uoou.cz* [online]. 2003 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/c-1-2003-monitorovani-elektronicke-posty-a-ochrana-soukromi-a-osobnich-udaju-zamestnancu/ds-2551/archiv=0&p1=2515

2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pojem zpracování je spolu s definicí osobního údaje klíčovým pro problematiku ochrany osobních údajů. Zákonné povinnosti se totiž vztahují pouze na takové nakládání s osobními údaji, které je ve smyslu § 4 písm. e) zákona o ochraně osobních údajů zpracováním. Definice tohoto pojmu byla do zákona o ochraně osobních údajů převzata ze směrnice 95/46/ES, popř. z Úmluvy č. 108, v níž můžeme najít jen drobné rozdíly.

Zákon vymezuje zpracování jednak obecně, ale i demonstrativním výčtem případů, kdy ke zpracování může dojít. Obecně je zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky.[26]

Důležitým prvkem je systematičnost zpracování. Tento požadavek je však specifikem českého zákona, ve směrnici 95/46/ES se nevyskytuje. Zákon o ochraně osobních údajů tento pojem nijak nedefinuje, přestože je pro tuto úpravu klíčový. Zatímco automatické zpracování bude probíhat systematicky vždy, problém může nastat v případě manuálního zpracování, kdy je nutno prověřit, zda se nejedná jen o nahodilý úkon, kterýžto by do působnosti zákona o ochraně osobních údajů nespadal.[27] Za zpracování tedy můžeme považovat jen ty operace, které jsou prováděny opakovaně, u kterých existuje úmysl je opakovaně provádět, nebo operace, u nichž je předpoklad jejich pokračování. Mohlo by tedy jít například o vedení databáze, rejstříku, kartotéky, registru apod.

V případě pracovněprávních vztahů budou za systematické zpracování považovány veškeré operace prováděné s osobními údaji obsaženými v životopisech uchazečů o zaměstnání, a to od okamžiku jejich převzetí správcem až po jejich zařazení do konkrétního registru.

V demonstrativní části definice se zpracováním osobních údajů rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. Tento příkladný výčet je zcela úmyslný, aby zákonodárce při každém technickém

[26] § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[27] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 23.

pokroku nemusel zákon novelizovat. Pro zpracování ve smyslu znění zákona o ochraně osobních údajů není podstatné, zda správce či zpracovatel učiní pouze jeden nebo více úkonů.[28]

2.1 Způsoby zpracování osobních údajů

Některé definice operací, které jsou za zpracování osobních údajů považovány, můžeme najít v ustanovení § 4 zákona o ochraně osobních údajů. V této podkapitole bych se ráda zaměřila na některé z nich a podrobněji je vysvětlila.

Prvním ze způsobů zpracování je shromažďování. Tím je systematický postup nebo soubor postupů, jehož cílem je získat osobní údaje za účelem uložení na nosič informací pro jejich okamžité či pozdější zpracování.[29] Tato činnost musí probíhat systematicky, tedy se záměrem dosáhnout určitého uspořádání souboru, nebo pomocí technických prostředků uspořádání docílit. Není důležité, zda se tak děje soustavně či ojediněle ani pomocí jakých prostředků je tohoto dosaženo. O shromažďování půjde již v okamžiku, kdy je získán první údaj. Shromažďováním je tedy záměrná činnost, jejímž cílem je získat údaje a informace a udržet si je na jakémkoli nosiči informací, přičemž ten není zákonem definován. Může tak jít o jakýkoli materiál, který bude schopen danou informaci uchovat. Podstatou shromažďování je tedy možnost získané informace dále zpracovávat, přičemž tato možnost není nijak limitována. S údaji tedy může být dále nakládáno bezprostředně po jejich nashromáždění nebo také s větším časovým odstupem.[30]

Dalším způsobem zpracování je uchování, neboli udržování osobních údajů v takové podobě, ve které bude možné jejich další zpracování. Možnost tyto údaje zpracovat pak musí trvat po celou dobu jejich uchování. Uchovávání je pak definováno v ustanovení § 4 písm. g) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění platném od 1. července 2017. Volba nosiče údajů, resp. způsobu jejich uchování je základním kritériem pro určení, o jaký další způsob zpracování půjde. Listinná forma bude znamenat zpracování manuální, zatímco uchování na technickém záznamovém médiu bude

[28] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 23.
[29] § 4 písm. f) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[30] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 24.

předpokladem pro zpracování automatizované. Způsob uchování údajů se může v průběhu času měnit (například převedení informací z listinné do elektronické podoby). Není pak podstatné, jestli bude nosič informací vlastnictvím správce, nebo zda bude k uchovávání docházet u zpracovatele či jiné osoby. Příkladem takového uchování údajů může být cloud, neboli sdílené datové úložiště.

Třetím způsobem je tzv. blokování, což je specifická a většinou jednorázová operace dočasné povahy, jejíž definice je obsažena v ustanovení § 4 písm. h) zákona o ochraně osobních údajů. Je jím operace nebo soustava operací, kterými se na danou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů. Správce tedy bude moci provádět i v případě blokování takové zásahy či operace, jejichž neprovedení by pro ochranu a integritu dat a ochranu soukromí dotčených osob znamenalo výrazně větší zásah do soukromí, než jejich provedení v daném omezeném režimu. Půjde tedy zejména o plnění povinností, které jsou správcům ustanoveny zněním § 13 zákona o ochraně osobních údajů, tj. povinnost zabezpečit zpracovávané osobní údaje před změnou, zničením, ztrátou, zneužitím apod. Správci z ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů vyplývá obecná povinnost osobní údaje blokovat, jestliže zjistí, že zpracovávané osobní údaje nejsou s ohledem na účel zpracování přesné. Správce je v takovém případě povinen nepřesné údaje nejen blokovat, ale následně také opravit, doplnit či zlikvidovat. Na toto navazuje ustanovení § 21 odst. 1 téhož zákona, které zakotvuje právo subjektu osobních údajů podat námitku. Tento paragraf říká, že: „k*aždý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může požádat správce nebo zpracovatele o vysvětlení nebo požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav.“*

Čtvrtým způsobem zpracování osobních údajů je likvidace, upravená § 4 písm. i) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění platném od 1. července 2017. Ta se vztahuje na data v listinné i elektronické podobě. Likvidací se rozumí taková operace, jejímž důsledkem je nevratné zničení uchovávaných, resp. zpracovávaných informací, přičemž tímto krokem je zpracování ukončeno. Operace spočívá ve fyzickém zničení nosiče, jeho vymazání nebo trvalém vyloučení ze zpracování. Je úkonem

nevratným a vztahuje se na veškeré osobní údaje, ne jen na ty, pomocí nichž by byla možná identifikace subjektu, jak tomu je v případě anonymizace. Za likvidaci by tedy nebylo možné považovat takový způsob, po jehož provedení by bylo možné, kupříkladu s pomocí využití jiných technických prostředků, tyto údaje obnovit tak, aby měly opět podobu údajů osobních.[31]

Za způsob zpracování je považováno také předávání osobních údajů, které spočívá v přenosu osobních údajů mezi správcem a příjemci, resp. mezi správcem a zpracovatelem. Zvláštním případem je pak přenos osobních údajů mimo území ČR, tj. předání osobních údajů správci nebo zpracovateli v jiném státě, což je podrobněji upraveno v § 27 zákona o ochraně osobních údajů, a to včetně podmínek pro přenos a zákazu omezení volného pohybu osobních údajů v EU.

2.2 Subjekt údajů

To, kdo je za subjekt údajů považován, můžeme vyčíst z několika věcí. Už z názvu směrnice 95/46/ES, neboli směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, vyplývá povinnost členských států zajistit ochranu základních práv a svobod všem fyzickým osobám, zejména práva na ochranu jejich soukromí v souvislosti se zpracováním osobních údajů.[32] Úmluva č. 108 ve svém článku 1 taktéž stanoví jako svůj účel existence zaručení práva na respektování základních lidských práv a svobod, zejména pak právo na soukromý život každé fyzické osoby. Právnická osoba, jakožto osoba fiktivní, uměle vytvořená, sice disponuje právní subjektivitou, ta se však nepromítne do sféry soukromé. Z toho vyplývá, že právnická osoba nemá soukromí, které by bylo zapotřebí chránit. Na tuto oblast by se pak vztahovala problematika vymezená v článku 1 odst. 2 směrnice 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, který říká, že *„ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES pro účely uvedené v odstavci 1. Navíc poskytují ochranu oprávněných zájmů účastníků, kteří jsou právnickými osobami.“*

[31] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 27.
[32] Čl. 1 odst. 1 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.

Další problém nastává v případech nascitura, osob zemřelých a osob fyzických podnikajících.[33] Podle ustanovení § 23 zákona č. 89/2012 Sb., zákon občanský zákoník (dále jen občanský zákoník), je subjektem údajů člověk, který má právní způsobilost od narození do smrti. V některých případech se na již počaté ale dosud nenarozené dítě, neboli nasciturus, hledí jakoby již narozeno bylo, vyhovuje-li to jeho zájmům. Narozením se tak stává nositelem práv a povinností. To však jen za předpokladu, že se následně dítě narodí živé, přičemž za něj dočasně danou způsobilost vykonává zákonný zástupce.[34] Navzdory ustanovení § 23 ponechává Úřad pro ochranu osobních údajů jistá práva i zesnulým.[35]

Za subjekt údajů je dle legální definice považována fyzická osoba, k níž se osobní údaje vztahují.[36] Jak již bylo řečeno dříve, zákon o ochraně osobních údajů se vztahuje pouze na osoby fyzické, nikoli na osoby právnické. Problém však nastává v případě podnikajících fyzických osob, které mohou i nemusejí být subjektem údajů. Názory Ústavního soudu a Evropských soudů se zde rozcházejí. Ústavní soud ve svém nálezu sp. zn. Pl. ÚS 38/02 ze dne 9. března 2004 konstatoval, že: „*o fyzických osobách, které jsou podnikateli, lze usuzovat stejně jako o právnických osobách, neboť z hlediska jejich statusu je nutno za rozlišovací kritérium považovat jejich podnikatelskou činnost.“* Evropské soudy naproti tomu zastávají názor, že u fyzických osob podnikajících je soukromí a profesní život úzce svázán a někdy je nelehké tenkou hranici mezi nimi odlišit.[37] Osobně se domnívám, že jsou-li zpracovávány pouze údaje související s podnikáním, pak by se na ně zákon o ochraně osobních údajů vztahovat neměl, protože podnikání nepatří mezi činnosti, jež by neoprávněně zasahovaly do soukromí. Fyzická osoba si podnikání jako svou činnost svobodně a dobrovolně vybrala, musí se tedy smířit s určitým zásahem do soukromí či jeho případným omezením. Zároveň si také myslím, že pokud by spadaly fyzické osoby podnikající do zákona o ochraně osobních údajů, nebylo by to v pořádku vůči osobám právnickým, které jsou z působnosti tohoto zákona vyňaty.

[33] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 106.
[34] § 25 zákona č. 89/2012 Sb., občanský zákoník.
[35] Stanovisko č. 4/2012 – Zpracování osobních údajů zemřelých osob. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/files/stanovisko_2012_4_old.pdf
[36] § 4 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[37] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 109.

2.3 Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů je jednostranným právním jednáním, jímž projevuje subjekt údajů svou vůli tím, že poskytne souhlas k zásahu do jeho soukromí konkrétním zpracováním jeho osobních údajů. Náležitosti právního jednání jsou stanoveny ustanoveními občanského zákoníku, konkrétně ustanoveními § 545 až § 564, která tento akt označují za projev vůle směřující zejména ke vzniku, změně nebo zániku těch práv nebo povinností, které právní předpisy s projevem spojují. Rovněž musí být právní jednání učiněno svobodně a vážně, určitě a srozumitelně. Nesplňoval-li by projev vůle zákonné náležitosti, jednalo by se o projev neplatný. Kromě náležitostí obsažených v občanském zákoníku zde existuje i požadavek vyplývající ze zákona o ochraně osobních údajů, aby byl projev vůle vědomý.

Za svobodný by byl považován takový projev vůle, který by byl subjektem údajů udělen bez působení takových vnějších vlivů, jež by omezovaly jeho možnost se samostatně rozhodnout, zda souhlas udělí či nikoli. Svoboda jednání by byla porušena za předpokladu donucení subjektu k udělení souhlasu, například donucení zaměstnance dát souhlas ke zpracování údajů, jež by se nevztahovaly k výkonu jeho povolání nebo ke kamerovému sledování, pod pohrůžkou ukončení pracovního poměru atd. Byl-li by pak souhlas udělen například v žertu nebo na zkoušku, nebyl by splněn požadavek vážnosti tohoto projevu vůle a ten by byl následně považován za neplatný. Aby mohl subjekt údajů vědomě projevit svou vůli, musí vědět, k čemu se zavazuje, resp. k jakému zpracování své osobní údaje poskytuje. Informovanost souhlasu je taktéž podmínkou jeho platnosti, s čímž souvisí povinnost správce údajů informovat subjekt podle ustanovení § 5 odst. 4 a § 11 odst. 1 a 2 zákona o ochraně osobních údajů.

Aby bylo právní jednání považováno za platné, musí být taktéž učiněno náležitou osobou. Nejčastěji je souhlas se zpracováním osobních údajů poskytován přímo subjektem údajů. V případě udělení souhlasu osobou neoprávněnou, nemůže na něj být brán zřetel. Existuje zde však možnost udělení souhlasu prostřednictvím zástupce, je však nutné zmocnění na základě zákona či plné moci. Zástupce tedy v rámci pravomocí, které mu byly svěřeny, může poskytnout souhlas se zpracováním osobních údajů za subjekt, jehož se údaje týkají a který jej zmocnil. Za děti pak poskytují souhlas se zpracováním osobních údajů jejich zákonní zástupci, nejčastěji rodiče. Zde se však nabízí otázka,

jak posuzovat souhlas se zpracováním osobních údajů u osob sice nezletilých, ale blížících se věku zletilého. Podle § 31 občanského zákoníku se má za to, že: *„každý nezletilý, který nenabyl plné svéprávnosti, je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jeho věku.“* Požaduje-li tedy správce souhlas se zpracováním od nezletilého, musí pečlivě zvážit, zda je nezletilý schopný, vzhledem ke své rozumové a volní vyspělosti, požadovaný souhlas udělit. Jinak řečeno musí uvážit, zda je dotyčný nezletilý schopen posoudit všechny aspekty zamýšleného zpracování. Pro správce může být výhodnější, především ve složitějších otázkách a z důvodu právní jistoty, požadovat kromě souhlasu nezletilého i souhlas jeho zákonného zástupce. Zároveň si však myslím, že souhlas nezletilého, ve věku blížícím se zletilému, nelze v žádném případě plně nahradit souhlasem zákonného zástupce, jestliže nezletilý s udělením souhlasu se zpracováním výslovně nesouhlasí. Pokud tedy není souhlas učiněn oprávněnou osobou nebo nesplňuje-li potřebné náležitosti, kdy musí být učiněn svobodně, vážně, určitě a srozumitelně, měl by být považován za absolutně neplatný, a to už od počátku, a zpracování na něm založené by mělo být posouzeno jako protizákonné.

Souhlas se zpracováním osobních údajů nemusí být vždy udělen výslovně, může se jednat i o konkludentní právní jednání. Poskytne-li tedy subjekt své údaje správci a ten ho informuje o jeho úmyslu je dále zpracovávat, není nutné dalšího souhlasu k jejich zpracování. Poskytnutí údajů v případě informovanosti subjektu zcela postačí. S dostatečností konkludentního souhlasu však koliduje povinnost správce být schopen po celou dobu zpracování osobních údajů prokázat existenci souhlasu subjektu údajů, proto rozhodně nemůže být na škodu, když si správce opatří i souhlas výslovný. Výslovný souhlas je však, podle zákona o ochraně osobních údajů, vyžadován vždy v případě zpracování citlivých údajů.[38]

Podle směrnice 95/46/ES je za souhlas subjektu považován jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, jež se ho týkají, byly předmětem zpracování.[39] V návaznosti na to je platnost souhlasu upravena i ve směrnici 2002/58/ES, kde je souhlas považován za platný v případě splnění čtyř kritérií. Souhlas tedy musí být jasným a jednoznačným projevem vůle, musí být dán svobodně, specificky

[38] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 92.

[39] Čl. 2 písm. h) 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.

a informovaně.[40] Souhlas se zpracováním musí být vždy udělen ještě před započetím zpracování.

Souhlas se zpracováním nemůže a nesmí být v žádném případě podmínkou, jež by sama o sobě, v případě jeho neudělení, znemožňovala uzavření smluvního vztahu. Podle stanoviska Úřadu pro ochrnu osobních údajů č. 2/2011 je souhlas se zpracováním osobních údajů považován za jednostranný projev vůle subjektu údajů, a ne dvoustrannou smlouvu mezi správcem a subjektem údajů. Souhlas se zpracováním tedy nelze zařadit mezi smluvní ujednání, neboť subjekt údajů nad rámec vlastního smluvního vztahu souhlasí, aby správce použil jeho osobní údaje za stanoveným účelem. Stanovisko vychází z ustanovení § 5 odst. 2 písm. b) zákona o ochraně osobních údajů, které říká, že souhlasu subjektu údajů není třeba, je-li zpracování osobních údajů nutné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů nebo pro jednání o uzavření nebo změně smlouvy, které je uskutečněno na základě návrhu subjektu údajů.[41] Souhlas je nejčastěji správci vyžadován pro případy zpracován osobních údajů v souvislosti s marketingovými účely nebo pro účely vedení registru dlužníků.

Úřad pro ochranu osobních údajů shrnul své názory týkající se náležitostí souhlasu se zpracováním osobních údajů ve svém stanovisku č. 2/2008. Aby byl souhlas se zpracováním osobních údajů platný, musí splňovat následující náležitosti. Právní jednání musí být učiněno svobodně, vážně, určitě a srozumitelně. Ten, kdo souhlas poskytne, musí být předem informován, za jakým účelem, kým, na jak dlouho a jaké konkrétní osobní údaje budou zpracovávány. V případě zpracování citlivých osobních údajů musí být dán souhlas výslovný, jak již bylo řečeno výše. Souhlas musí být prokazatelný po celou dobu trvání zpracování.[42]

V případě pracovněprávních vztahů je podstatné ustanovení § 316 zákona č. 262/2006 Sb., zákoníku práce, které ve svém odst. 2 říká, že: *„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo*

[40] Čl. 9 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).
[41] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související*: komentář. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 125.
[42] Stanovisko č. 2/2008 – Souhlas se zpracováním osobních údajů. *Uoou.cz* [online]. 2008 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/files/stanovisko_2008_2.pdf

skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“ Odstavec třetí pak konstatuje, že: *„jestliže má zaměstnavatel závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění“*. Od těchto ustanovení se nelze odchýlit, neboť mají kogentní povahu.[43] K této problematice se také vyjádřila pracovní skupina „WP 29“ ve svém stanovisku č. 8/2001, kde konstatovala, že zpracování osobních údajů v rámci pracovněprávních vztahů na základě souhlasu by se mělo omezit zásadně na situace, ve kterých má zaměstnanec skutečně svobodnou volbu s postupem zaměstnavatele nesouhlasit a možnost následně svůj souhlas odvolat, a to bez jakýchkoli následků. V situaci, kdy je zaměstnanec žádán o poskytnutí souhlasu se zpracováním osobních údajů, přičemž ale existuje riziko jakékoli újmy v případě odmítnutí souhlasu, nelze ani udělený souhlas považovat za platný právní úkon.[44]

Problematika odvolatelnosti není v zákoně o ochraně osobních údajů upravena, avšak lze logicky dovodit, že odvolání možné je. V tomto případě by se však podle mého názoru dala použít analogie podle ustanovení § 87 odst. 1 občanského zákoníku, které říká, že: *„kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu.“* V případě důsledků odvolání souhlasu na dobu určitou by pak byl použit odstavec 2 stejného paragrafu, který říká, že: *„Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.“*

Souhlasu subjektu údajů ke zpracování pak není třeba v případech uvedených v ustanovení § 5 odst. 2 zákona o ochraně osobních údajů. Jde například o případy, kdy je zpracování nezbytné pro dodržení právní povinnosti správce, je-li to nezbytné pro plnění, uzavření nebo změnu smlouvy, jejímž signatářem je subjekt údajů nebo jedná-li se o oprávněně zveřejněné osobní

[43] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 83/06 ze dne 12. 3. 2008.
[44] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 131.

údaje v souladu se zvláštním právním předpisem a v dalších případech podle uvedeného ustanovení.

2.4 Správce

Správce je jedním z klíčových pojmů pro oblast ochrany osobních údajů. Je jím podle definice nalézající se ve směrnici 95/46/ES článek 2 písm. d) ten, kdo je *„fyzickou nebo právnickou osobou, orgánem veřejné moci, agenturou nebo jakýmkoli jiným subjektem, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů; jsou-li účel a prostředky zpracování určeny právními a správními předpisy na úrovni jednotlivých států či Společenství, je možné určit správce nebo zvláštní kritéria pro jeho určení právem jednotlivých států nebo Společenství“*. Toto znění bylo implementováno do českého práva prostřednictvím ustanovení § 4 písm. j) zákona o ochraně osobních údajů, kterým je za správce považován každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Tento paragraf doplňuje znění § 3 odst. 1 zákona o ochraně osobních údajů, podle něhož se tento zákon vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci a fyzické a právnické osoby. Dalo by se tedy říci, že se zákon o ochraně osobních údajů vztahuje na každého, kdo by osobní údaje zpracovával, bez ohledu na to, zda se jedná o právnickou či fyzickou osobu nebo státní orgán.

Mezi správce patří každý, kdo v rámci své činnosti zpracovává osobní údaje ve smyslu § 4 písm. e) zákona o ochraně osobních údajů. Jde tedy o ty, kteří například systematicky spravují databázi svých obchodních partnerů, zákazníků, klientů, pacientů apod. Zpracování může provádět správce sám nebo tím může někoho pověřit či zmocnit, není-li zvláštním zákonem stanoveno jinak. Tato osoba se nazývá zpracovatel (viz kapitola 2.5). Účel zpracování musí být na prvním místě legální, pokud je tedy dané zpracování stanovené zákonem, odvíjí se legalita od tohoto ustanovení. Pokud účel zpracování stanoven není a ani jej nelze odvodit od podmínek uvedených ve zvláštním zákoně, pak účel zpracování určuje správce sám. Pro posouzení legality je pak nutné[45] správce rozdělit do dvou kategorií, subjekt soukromoprávní a veřejnoprávní.

[45] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 78.

Soukromoprávní subjekt si v podstatě účel zpracování osobních údajů určuje sám, nejde-li o zpracování, které je určené zákonem. V zásadě tedy může činit to, co mu zákon nezakazuje. Po zvolení účelu si správce volí způsob a prostředky zpracování. Musí však dbát na to, aby šlo o způsob adekvátní vůči stanovenému účelu. Nebylo-li by to tak, pak by zpracování nadbytečně zasahovalo do soukromí a práv subjektů údajů a Úřad pro ochranu osobních údajů by mohl uplatnit své dozorové kompetence a v rámci své kontrolní pravomoci uložit správci opatření k nápravě až zakázání zpracování osobních údajů.

Subjekt veřejnoprávní může činit jen to, co je mu zákonem umožněno, a to pouze zákonem stanoveným způsobem. Výjimkou by byla situace, kdy by veřejnoprávní subjekt vystupoval jako soukromoprávní, například jako vlastník bytového domu a pronajímatel jednotlivých bytů apod. Typickým příkladem, kdy je zpracování správci uložené zákonem je zpracování osobních údajů v pracovněprávní oblasti, kde musí zaměstnavatelé vést řadu evidencí osobních údajů zaměstnanců, kupříkladu evidenci pracovní doby, účty mezd zaměstnanců aj. Provádí-li tedy správce, jakožto veřejnoprávní subjekt, zpracování osobních údajů v souladu s ustanoveními zákona, které mu to umožňují, nemůže se nikdy jednat o nelegální či neoprávněný zásah do soukromí. Vzhledem k tomu, že se veřejnoprávní subjekt od ustanovení zákona nemůže nijak odchýlit, musí využít způsob a prostředky zpracování osobních údajů stanovené zákonem i v případě, kdy by byly neadekvátní. Z toho vyplývá, že Úřad pro ochranu osobních údajů by nemohl uplatnit své dozorové kompetence jako v předchozím případě, ale musel by na nevhodné využití prostředků upozornit jinak, a to především proto, že není nadán zákonodárnou iniciativou.[46] Správce tedy musí v tomto případě dbát výběru prostředků zpracování jen v případě, kdy mu zákon umožňuje výběr z několika variant. Potom by Úřad pro ochranu osobních údajů (dále jen „Úřad“) svou dozorčí pravomoc uplatnit mohl, avšak nemohl by zakázat zpracování zcela, mohl by pouze v konkrétním případě zakázat tu z variant zpracování, která by se ukázala být příliš invazivní pro daný účel zpracování.

Správce plně odpovídá za legálnost zpracování. Na straně jedné má správce deliktní odpovědnost, která spočívá v možnosti uložení sankce Úřadem v případě porušení zákonných povinností správce. Na straně druhé má správce

[46] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 116.

vůči subjektu údajů odpovědnost soukromoprávní, subjekt tak může po správci vymáhat náhradu škody nebo nemajetkové újmy, která mu vznikla v rámci nelegální činnosti správce.

2.5 Zpracovatel

Zpracovatel je ustanovením směrnice 95/46/ES článku 2 písm. e) vymezen jako: „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce*“. Český zákonodárce pak toto ustanovení převzal a zjednodušil do ustanovení § 4 písm. k) zákona o ochraně osobních údajů, který říká, že: „*zpracovatelem je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona*“. V českém prostředí jsou na zpracovatele dále kladeny velmi striktní požadavky. Povinnosti zpracovatele jsou upraveny v § 7 zákona o ochraně osobních údajů, který zde stanovuje, že veškeré povinnosti správce popsané v § 5 daného zákona platí obdobně i pro zpracovatele.

Zpracovatel však na rozdíl od správce neurčuje účel ani prostředky zpracování osobních údajů, pouze provádí zpracování osobních údajů jako takové. Nemusí provádět zpracování od počátku až do konce, nýbrž může provádět jen některé dílčí činnosti, které se zpracováním souvisí. Může zpracovávat osobní údaje na základě výslovného zákonného zmocnění, na základě zmocnění správcem nebo na základě smluvního ujednání. Smlouva o zpracování mezi správcem a zpracovatelem musí mít všechny náležitosti stanovené v § 6 zákona o ochraně osobních údajů, který upravuje její formu, rozsah, účel a dobu trvání této smlouvy, dále také záruky zpracovatele o zabezpečení zpracovávaných údajů.

Zpracovatel není zaměstnancem správce ani jeho vnitřním útvarem, ale vždy odlišnou osobou, která pro správce určité části či celé zpracování provádí.[47] Není tedy možné, aby byl subjekt správcem údajů i zpracovatelem současně. Možné by to bylo pouze v případě, kdy by zpracovatel zpracovával informace poskytnuté od správce i k jiným, vlastním účelům, avšak k tomu by potřeboval vlastní a samostatný právní titul. Samotné zpracování musí zpracovatel provádět na základě pokynů od správce a v souladu s právními předpisy.

[47] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 82.

Zpracovatel může také na základě uzavřené smlouvy za správce činit i další úkony, jako je např. informační nebo oznamovací povinnost. Podobně jako správce, i zpracovatel sám za zpracování odpovídá. Je odpovědným subjektům zpracovávaných údajů. Dojde-li při zpracování k porušení zákona, odpovídají správce a zpracovatel za způsobenou škodu společně a nerozdílně, neboli solidárně, podle § 21 odst. 4 zákona o ochraně osobních údajů. Subjekt údajů se může v takovém případě sám rozhodnout, po kom bude v daném případě náhradu škody vymáhat. Případný regresní nárok mezi správcem a zpracovatelem bude probíhat dle ustanovení občanského zákoníku. Zpracovatel je dále odpovědný vůči správci v případě porušení smlouvy o zpracování. Zpracovatel může být také, podobně jako správce, odpovědný ze spáchání přestupku či správního deliktu podle zákona o ochraně osobních údajů. Zpracovatel nemůže obecně svou povinnost vyplývající ze smlouvy o zpracování, kterou uzavřel se správcem, převést na někoho jiného bez souhlasu správce. Avšak na základě § 14 zákona o ochraně osobních údajů, může zpracovatel využít služeb jiných osob, jak fyzických tak právnických, s nimiž má uzavřenou pracovní či jinou obdobnou smlouvu.[48]

2.6 Příjemce

Podle směrnice 95/46/ES článku 2 písm. g) je příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, kterému jsou údaje sdělovány, ať se jedná o třetí osobu či nikoli; orgány, které mohou získávat údaje v rámci zvláštního šetření, však nejsou považovány za příjemce. V původním znění zákona o ochraně osobních údajů nebyla definice příjemce obsažena. Ta byla přidána až novelizací, která byla provedena zákonem č. 439/2004 Sb. Tato definice tedy v zákoně přibyla, podle důvodové zprávy se tak stalo z důvodu ustanovení výše zmíněného článku směrnice 95/46/ES, protože nastala nutnost definovat příjemce jako další osobu, resp. subjekt, kterému mohou být zpracovávané osobní údaje zpřístupněny, předány atd.[49]

Bude-li příjemce získané údaje dále sám o své vůli zpracovávat, bude se jednat o odlišné a samostatné zpracování a příjemce se tak sám stane správcem

[48] Stanovisko č. 1/2009 – Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/stanovisko-c-1-2009-zpracovani-osobnich-udaju-na-zaklade-smluv-uzaviranych-se-zpracovateli-tzv-retezeni-zpracovatelu-osobnich-udaju/d-1509

[49] Ust. § 4 písm. o) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

s plnou odpovědností za toto zpracování a bude tak muset naplnit i všechny povinnosti, které správci zákon o ochraně osobních údajů přisuzuje. Za příjemce nebudou považovány ty osoby, jimž jsou osobní údaje zpřístupněny při výkonu kontroly, dozoru, dohledu a výkonu veřejné moci, podle ustanovení § 3 odst. 6 písm. g) zákona o ochraně osobních údajů. Tím, že jsou tyto subjekty vyčleněny z definice příjemce, je správce, popř. zpracovatel zbaven povinnosti o nich vést evidenci nebo o nich zpřístupňovat informace v rámci jejich povinnosti dle § 11 a § 12 zákona o ochraně osobních údajů.[50]

2.7 Povinnosti související se zpracováním

Zákon o ochraně osobních údajů stanoví pro správce a zpracovatele celou řadu povinností. Většina z nich je upravena v § 5 zákona o ochraně osobních údajů, avšak další povinnosti můžeme najít i v ustanoveních § 11 až § 13 a § 16 téhož zákona.

2.7.1 Stanovení účelu, prostředku a způsobu zpracování § 5

Je několik povinností, které správce musí split ještě před započetím zpracování osobních údajů. Zaprvé musí správce stanovit účel, resp. důvod, z jakého chce dané osobní údaje zpracovávat. Stanovení účelu patří mezi nejzákladnější a nejdůležitější povinnosti správce. Je to také jedna z věcí, která odlišuje správce od zpracovatele. Účel buďto vyplývá přímo ze zákona nebo ho z jeho ustanovení lze odvodit, není-li účel v zákoně obsažen, určuje ho správce sám. Dochází k tomu například u pracovněprávních vztahů v případě zákonné povinnosti zaměstnavatele vést evidenci pro účely nemocenského a důchodového pojištění[51] nebo povinnosti zaměstnavatele vést evidenci pracovní doby podle zákoníku práce.[52]

Účel musí být stanoven konkrétně, nikoli obecně, aby bylo možné zjistit, zda je legální a legitimní. Legitimním by bylo například opatření soukromých telefonních čísel zaměstnanců záchranné služby zaměstnavatelem pro jejich lepší dosažitelnost v případě sjednané pracovní pohotovosti aj.[53]

[50] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 93.
[51] Ust. § 37 a § 38 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení.
[52] Ust. § 96 zákona č. 262/2006 Sb., zákoník práce.
[53] Srov. NOVÁKOVÁ, L. in KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů: komentář*. Vyd. 1. Praha: C.H. Beck, 2012. ISBN 978-80-7179-226-0, s. 103–106.

Se stanovením účelu by měl správce současně určit i prostředky a způsoby, kterými chce stanoveného cíle dosáhnout. Oboje by mělo být stanoveno také ještě před započetím zpracování. Způsob i prostředky se však mohou v průběhu zpracování měnit, především z důvodu vhodnosti či efektivity. V některých případech může být oboje stanoveno zákonem, to se však děje jen velmi ojediněle. Způsob zpracování může být buďto automatizovaný nebo manuální, popř. jejich kombinace. Prostředek pak vypovídá o konkrétním nástroji, jehož bude třeba pro zpracování použít.

Všechny tyto povinnosti mají být důležitým nástrojem minimalizování zásahů do soukromí subjektů údajů. Správce může shromažďovat jen ty osobní údaje, které odpovídají účelu, a to jen v nezbytném rozsahu, nesmí tedy zpracovávat údaje zjevně nadbytečné. Cílem je dosažení situace, kdy bude účelu zpracování dosaženo za použití co nejužší skupiny osobních údajů. Správce je také povinen zpracovávat a uchovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny, k jinému účelu lze údaje zpracovávat jen v případech podle ustanovení § 3 odst. 6 zákona o ochraně osobních údajů nebo na základě souhlasu subjektu údajů. Z výše uvedeného plyne skutečnost, že subjekt údajů by měl být tím, kdo ve většině případů o zpracování svých osobních údajů rozhoduje a tím, kdo má o přehled minimálně o tom, jak je s jeho osobními údaji nakládáno, a to i v případech, kdy mu rozhodování o samotném zpracování nepřísluší. Správci je taktéž zakázáno, aby dohromady sdružoval osobní údaje, jež byly shromážděny k rozdílným účelům.[54]

Zjistí-li správce, že osobní údaje nejsou za daným účelem zpracovávány přesně, je povinen zpracování blokovat a nepřesné údaje ihned opravit nebo doplnit. Je tedy zřejmé, že správce je povinen zabezpečit a přijmout taková opatření, aby zajistil, že zpracovávané údaje budou přesné a aby k jejich získání a zpracování docházelo v souladu se zákonem o ochraně osobních údajů. Tento zákon také požaduje, aby byla prováděna aktualizace zpracovávaných osobních údajů, je-li to k účelu zpracování nezbytné a aby bylo případným nepřesnostem předcházeno, popř. aby došlo k nápravě nepřesností.

Správci je povoleno podle ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů uchovávat osobní údaje pouze po dobu, která je nezbytná pro dosažení účelu jejich zpracování. Po uplynutí této doby mohou být

[54] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 31–37.

osobní údaje nadále uchovávány jen pro účely statistické, vědecké či archivní, v takovém případě je však nutno je co nejdříve anonymizovat, aby nedocházelo k nadbytečnému zásahu do soukromí subjektů údajů. Správce je ve většině případů oprávněn sám rozhodnout o délce zpracování, vykonává-li však tuto činnost na základě zákonného zmocnění, může údaje uchovávat jen po dobu, kdy je mu tato povinnost vlastní.

Nakonec má správce povinnost shromažďovat osobní údaje pouze otevřeně, je přísně zakázáno osobní údaje shromažďovat pod záminkou jiného účelu nebo činnosti. Skryté shromažďování osobních údajů správci, na něž se nevztahují výjimky uvedené v § 3 odst. 6 zákona o ochraně osobních údajů, by bylo v demokratické společnosti nelegitimní. Požadavek legitimity a otevřenosti zpracování osobních údajů je podepřen i ustanoveními směrnice 95/46/ES a Úmluvy č. 108, ve kterých je stanoven požadavek na korektnost, resp. poctivost zpracování osobních údajů. Příkladem porušení této povinnosti by mohla být například situace, kdy by zaměstnavatel pořizoval kamerový záznam svých zaměstnanců za účelem ochrany majetku, avšak jeho skutečným záměrem by bylo sledování dodržování pracovní doby zaměstnanců. Případ pořizování záznamů ze skryté kamery, splňoval-li by její provoz veškeré zákonné náležitosti, by však skrytým zpracováním nebyl.

Porušení povinností správce a zpracovatele vyplývajících z § 5 zákona o ochraně osobních údajů by naplňovalo skutkovou podstatu správního deliktu, resp. přestupku podle tohoto zákona, ty by pak projednával Úřad pro ochranu osobních údajů.[55]

2.7.2 Informační povinnost

Informační povinnost je upravena v § 11 a § 12 zákona o ochraně osobních údajů. Zatímco § 11 upravuje povinnost správce, resp. zpracovatele, poskytnout informace, jež se týkají zpracování osobních údajů ještě před jejich zpracováním, § 12 upravuje práva subjektů údajů na přístup k informacím, jež se jejich osobních údajů týkají, a správce je povinen jim je kdykoli v průběhu zpracování poskytnout.

Recitál 38 Směrnice 95/46/ES uvádí, že korektní zpracování údajů předpokládá, že subjekty údajů jsou informovány o probíhajícím zpracování

[55] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 128–130.

a že mají nárok, pokud jsou údaje získávány od nich, na přesné a úplné informace o okolnostech tohoto shromažďování. Ustanovení § 11 zákona o ochraně osobních údajů je důsledkem implementace článků 10 a 11 směrnice 95/46/ES, které upravují povinnosti správce v souvislosti s informováním subjektů údajů ohledně jejich zpracování podle toho, zda byly získány přímo od samotných subjektů, nebo jestli je poskytl někdo jiný.

Zákon o ochraně osobních údajů nestanoví žádný způsob, jak mají být informace poskytnuty, avšak ze zákona o ochraně osobních údajů vyplývá povinnost správce subjekt údajů při jejich shromažďování informovat. Aby bylo zpracování osobních údajů považováno za legitimní a legální, musí být prováděno otevřeně a transparentně. Informační povinnost podle § 11 je tedy plněna tím, že správce při shromažďování osobních údajů uvede rozsah zpracovávaných osobních údajů, nejlépe pak taxativním výčtem, a účel jejich zpracování. Dále musí být subjekt informován o tom, jakým způsobem budou osobní údaje zpracovávány, kdo bude zpracování provádět, včetně vlastní identifikace správce. Správce také musí identifikovat i jakékoli třetí osoby, kterým mohou být údaje zpřístupněny, a to včetně osob, pro které jsou osobní údaje určeny. Tato povinnost musí být splněna ještě před započetím zpracování osobních údajů.

Nesplnění informační povinnosti také zpochybňuje platnost souhlasu se zpracováním osobních údajů, protože nedostal-li subjekt údajů všechny relevantní informace, které se zpracování týkají, nemohl o udělení souhlasu kvalifikovaně rozhodnout, tudíž je souhlas se zpracováním podle zákona o ochraně osobních údajů považován za neplatný. Úřad pro ochranu osobních údajů ve věci 26/05/SŘ-OSČ, 50/05/SŘ-OSČ a věci 70/05/SŘ-OSČ připomenul, že správci osobních údajů plní svou informační povinnost obvykle prostřednictvím textu souhlasu se zpracováním osobních údajů uvedeném ve smlouvě nebo na příslušném formuláři či ustanovením v rámci všeobecných obchodních podmínek. Je zde však nutnost poskytnout subjektu údajů uvedené informace ve srozumitelné a přehledné formě. V případě, kdy by byly informace předány velmi komplikovanou formou prostřednictvím rozsáhlého dokumentu, popř. několika dokumentů, dalo by se o splnění informační povinnosti přinejmenším pochybovat.[56] Řádná informovanost subjektu je předpokladem pro to, aby ten mohl využívat svá práva, jako například právo na informace

[56] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 214.

v průběhu jejich zpracování, právo na námitku podle § 21 zákona o ochraně osobních údajů nebo právo podat proti správci žalobu o náhradu škody a nemajetkové újmy způsobenou nezákonným zpracováním osobních údajů.

Správce nepodléhá informační povinnosti v případě, kdy jsou všechny osobní údaje, jež chce zpracovávat, již známy. Informační povinnosti taktéž nepodléhají správci, jsou již vymezeny v § 3 odst. 6 zákona o ochraně osobních údajů, jimiž jsou např. ozbrojené sbory, orgány činné v trestním řízení, zpravodajské služby či kontrolní a dozorčí orgány, a to zejména z důvodu, že by informování subjektu údajů bylo v přímém rozporu s účelem a smyslem jejich zpracování, přičemž jejich informační povinnost je obvykle stanovena ve zvláštních předpisech. Z této povinnosti jsou dále vyjmuti správci, kteří zpracovávají osobní údaje výlučně pro statistické, vědecké a archivní účely, ale pouze v případě, že by informování všech subjektů údajů, jichž údaje budou zpracovávány, představovalo pro správce vynaložení neúměrného úsilí a nepřiměřených nákladů. Za správce může podle § 11 odst. 7 zákona o ochraně osobních údajů plnit zpracovatel, k čemuž může dojít třeba tehdy, kdy by zpracovatel prováděl za správce sběr osobních údajů a spolu s ním by tedy informoval subjekty.[57]

Zákon o ochraně osobních údajů však prokazatelnost poskytnuté informace výslovně nepožaduje, nechává tak na správci, aby v případě nutnosti prokázal, zda svou informační povinnost splnil. Domnívám se tedy, že by bylo pro správce vhodné postupovat v případě jejich informační povinnosti stejně, jako při obstarávání souhlasu se zpracováním, tedy aby si skutečnost, že svou informační povinnost splnil a informace subjektu poskytl, nechal prokazatelným způsobem potvrdit. Nesplnění informační povinnosti totiž zakládá odpovědnost správce za přestupek či jiný správní delikt podle § 44 odst. 2 písmena f) nebo § 45 odst. 1 písm. f) zákona o ochraně osobních údajů.

Pod informační povinnost správce také spadá nutnost poučení subjektu o tom, zda jsou mu osobní údaje poskytovány ke zpracování dobrovolně nebo na základě zvláštního zákona. Je-li subjekt povinen poskytnout údaje správci ze zákona, pak má správce povinnost informovat subjekt údajů o tom, jaké důsledky bude mít případné neposkytnutí osobních údajů ke zpracování.[58] Subjekt musí být taktéž informován, zda může odmítnout osobní údaje

[57] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 221.
[58] Tamtéž, s. 212.

poskytnout, například v případech, kdy by mohl způsobit nebezpečí trestního stíhání sobě nebo osobám sobě blízkým.[59] Správce je však povinen subjekt informovat jen v případě, získává-li osobní údaje přímo od něj.

Informační povinnost podle § 12 přímo souvisí s povinností dle § 11 zákona o ochraně osobních údajů. Zatímco § 11 upravuje informační povinnost správce, resp. zpracovatele pouze v okamžiku shromažďování osobních údajů, ustanovení § 12 subjektu údajů umožňuje získávat informace o jejich zpracování kdykoli v průběhu jejich zpracování. Poskytování těchto údajů rovněž souvisí s právy subjektu podle § 21, neboli s právem na opravu, vysvětlení nebo likvidaci osobních údajů.

Informace jsou poskytovány na základě žádosti subjektu údajů, správce je povinen je předat bez zbytečného odkladu, přičemž může za jejich poskytnutí požadovat přiměřenou úhradu nákladů nepřevyšující náklady nezbytné pro jejich poskytnutí.[60] Nárok na úhradu nákladů se však podle zákona vztahuje pouze na správce. Zpracovatel, ačkoli může za správce splnění informační povinnosti převzít, na náhradu nákladů nárok nemá. V takovém případě by zpracovatel musel požadovat náhradu nákladů přímo po správci, a to v souladu se smlouvou, na jejímž základě plní správcovu informační povinnost. Ten by pak mohl náhradu nákladů dodatečně požadovat po žadateli, resp. subjektu údajů.[61]

Zákon o ochraně osobních údajů neupravuje formu ani způsob, jakým má být žádost správci předána. Zatímco nejčastější bude jistě forma písemná, nelze vyloučit ani formu ústní. Dané ustanovení v odst. 3 mimo jiné určuje i konkrétní informace, které mají být subjektu údajů poskytnuty. Jde o informace o účelu zpracování osobních údajů, informace o zpracovávaných osobních údajích, popř. jejich kategoriích, informace o zdroji osobních údajů a informace o povaze automatizovaného zpracování.[62] V případě, že by správce odmítl požadovanou informaci vydat, může se subjekt se svou stížností obrátit na Úřad pro ochranu osobních údajů. Úřad by pak v návaznosti na provedené šetření případu mohl správci poskytnutí informace nařídit v rámci své kontrolní pravomoci, přičemž nesplnění této povinností je současně přestupkem, resp. správním deliktem.

[59] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 42.
[60] § 12 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[61] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 226.
[62] § 12 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

2.7.3 Zabezpečení osobních údajů § 13

Problematiku zabezpečení osobních údajů upravuje článek 17 směrnice 95/46/ES, který říká, že: „*členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování. Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny*.“ Znění článku 17 zmíněné směrnice bylo implementováno do ustanovení § 13 zákona o ochraně osobních údajů, který povinnost zabezpečení upravuje v českém právu. Povinnost zabezpečit osobní údaje upravuje také článek 7 Úmluvy č. 108. Tato povinnost zároveň patří mezi obecné povinnosti správce a zpracovatele, jejímž smyslem je chránit osobní údaje. Tato povinnost je realizována prostřednictvím stanovení pravidel pro bezpečnost zpracování osobních údajů, které mají údaje chránit před úmyslným a nedbalostním jednáním a před působením přírodních a jiných událostí, které by mohly zapříčinit zneužití osobních údajů. Tato povinnost patří mezi jednu z podmínek zpracování a její použitelnost není časově omezena. Dohlédnout na to, aby byly osobní údaje v bezpečí, musí správce, resp. zpracovatel nejen po dobu zpracování, ale i po jejím uplynutí. Zabezpečení tedy musí trvat po celou dobu, po kterou má správce zpracovávané údaje k dispozici, dokud nedojde k jejich anonymizaci nebo likvidaci.

Přijetí vhodných a zároveň dostatečných bezpečnostních opatření napomáhá minimalizovat zásah do soukromí subjektu údajů. O přijetí bezpečnostních opatření rozhoduje sám správce, přičemž je zcela na něm, aby přijal dostatečná bezpečnostní opatření odpovídající míře zabezpečení, která je potřebná pro zpracování daných osobních údajů. Zpracovává-li osobní údaje zpracovatel, pak je i on povinen příslušná opatření přijmout. Je nutné, aby hodnota, úsilí a odborná úroveň potřebná pro realizaci příslušného bezpečnostního opatření byla přinejmenším rovna jeho prospěšnosti a úrovni zabezpečení pro účely ochrany osobních údajů před riziky, za jejichž účelem byla bezpečnostní opatření přijata. Správce a zpracovatel odpovídají podle zákona

o ochraně osobních údajů za přijetí příslušných opatření, a to objektivně, tedy odpovídají za následek jednání i za opomenutí.

Zabezpečením se tedy ve smyslu § 13 rozumí „*povinnost správce a zpracovatele přijmout taková 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.*“ Zákon o ochraně osobních údajů nechává volbu prostředků zabezpečení zcela na správci, resp. zpracovateli, avšak podává v ustanovení § 13 odst. 3 a 4 příkladný výčet situací, proti kterým musí být osobní údaje chráněny. Při výběru je pak nezbytné přihlédnout i k výběru způsobu a prostředku zpracování. K naplnění skutkové podstaty správního deliktu podle § 46 odst. 1 v případě porušení povinnosti vyplývající z § 13 odst. 1 by stačil stav, kdy by z důvodu nepřijetí bezpečnostních opatření nastala situace, která by třeba jen umožnila neoprávněné zpracování osobních údajů, tj. pouhé ohrožení osobních údajů dává vznik již zmíněnému správnímu deliktu. Zpřístupnění osobních údajů třetí osobě je jen důsledkem nesplnění povinnosti přijmout příslušná opatření.[63] Je zde však možné využití liberačního důvodu, podle něhož fyzická či právnická osoba za spáchaný delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které po ní bylo možné spravedlivě vyžadovat, aby porušení právní povinnosti zabránila.[64]

Správce nebo zpracovatel je taktéž povinen zpracovat a dokumentovat všechna přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.[65] Porušení této povinnosti není podřaditelné pod žádný správní delikt podle § 44 a § 45, avšak může zavdat příčinu uložení opatření k nápravě podle § 40 daného zákona. V případě zabezpečení zpracovávání osobních údajů existuje nutnost, aby správce seznámil ty zaměstnance, kteří s osobními údaji přichází do styku, s podmínkami a pravidly, které musí v tomto styku dodržovat. Nezáleží pak na tom, jakou formou budou zaměstnanci o povinnostech informováni, avšak správce by měl být

[63] Z rozhodovací činnosti Úřadu. *Uoou.cz* [online]. s. 5–6, bod 6 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=5092
K dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů v soukromoprávní sféře. *Uoou.cz* [online]. 2013 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/k-dodrzovani-povinnosti-prijmout-a-provest-bezpecnosti-opatreni-k-ochrane-osobnich-udaju-v-soukromopravni-sfere/d-1598/p1=2855

[64] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 229.

[65] Ust. § 13 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

vždy schopen prokázat přijetí a provedení těchto opatření. Vymezení pravidel však samo o sobě nestačí, pokud správce nekontroluje jejich dodržování. V tomto případě leží dohlížení nad dodržováním odpovídajících povinností především na bedrech vedoucích zaměstnanců správce údajů.[66] Nebyl-li by správce schopen prokázat, že své zaměstnance řádně seznámil s pravidly zpracování, a zároveň dohlédl na to, aby byla dodržována, odpovídal by za všechna případná ohrožení, popř. zneužití osobních údajů sám.[67]

Do oblasti přijetí příslušných bezpečnostních opatření patří také povinnost mlčenlivosti, která je nejčastěji uložena osobám v pracovním nebo obdobném poměru u správce nebo zaměstnavatele a trvá i po skončení zaměstnání nebo přidělených prací. Tato povinnost se vztahuje nejen na samotné osobní údaje, ale také na příslušná bezpečnostní opatření, jejichž vyzrazení by ohrozilo zabezpečení osobních údajů.[68] Zavázal-li se zaměstnanec k mlčenlivosti podle § 15 zákona o ochraně osobních údajů a poruší-li ji, pak je odpovědný za spáchání přestupku podle § 44 odst. 1 zákona o ochraně osobních údajů, přičemž mu za jeho čin může být udělena pokuta až do výše 100 000 Kč.[69] Další povinností související se zabezpečením je povinnost již zmíněné likvidace podle § 20, kterou je nutno provést po ukončení zpracování osobních údajů, aby bylo zamezeno jejich případnému zneužití (viz kapitola 2.1).

2.7.4 Oznamovací povinnost

Oznamovací povinnost Úřadu pro ochranu osobních údajů patří mezi jednu ze základních povinností subjektu odpovědného za zpracování osobních údajů. Tuto povinnost je nutno splnit ještě před aktivním započetím zpracování osobních údajů. Zákon o ochraně osobních údajů v souladu s právem EU výslovně stanovuje obsah tohoto oznámení, avšak neupravuje jeho formu.

Tato primární povinnost obecně vyplývá z ustanovení § 16 odst. 1 zákona o ochraně osobních údajů, které je v přímém souladu s ustanovením článku 18 odst. 1 směrnice 95/46/ES. Český právní řád však nepřejal výjimky z oznamovací povinnosti, které uvádí tato směrnice. Jedná se zejména o možnost

[66] Ust. § 302 písm. f) zákona č. 262/2006 Sb., zákoník práce.
[67] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 44–50.
[68] Ust. § 15 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[69] Ust. § 44 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

vynětí subjektů, jež si zvolí osobu pověřenou ochranou osobních údajů, z oznamovací povinnosti. Úřad pro ochranu osobních údajů vede pro účely zveřejnění přijatých oznámení veřejně přístupný registr, v souladu s ustanovením § 29 odst. 1 písm. b) zákona o ochraně osobních údajů. Smyslem registrace je pak dle recitálů 48 až 53 směrnice 95/46/ES zejména zveřejnění účelu zpracování a jeho základních parametrů, aby mohla proběhnout v souladu s vnitrostátními předpisy jeho kontrola. Kontrola je zde pak prováděna nejen Úřadem, ale i veřejností.

Obsahově požaduje Úřad po budoucím správci oznámení o účelu zpracování, identifikační údaje správce, popis způsobu zpracování osobních údajů, informace o jejich zabezpečení a ochraně, místo zpracování, kategorie zpracovávaných osobních údajů a subjektu údajů, zdroje osobních údajů, případné příjemce a přeshraniční předání osobních údajů. U přeshraničního předání osobních údajů do cizích států je zásadní, zda jsou dané státy členy EU nebo ne, popř. jestli mají tyto státy s ČR uzavřenou smlouvu o ochraně osobních údajů nebo jestli jsou signatáři Úmluvy č. 108.

Úřad nabízí pro urychlení a zefektivnění oznamovacího procesu elektronický formulář, který je dostupný na jeho webových stránkách. Registrační formulář však slouží pro oznámení jen jediného zpracování, chystá-li se tedy správce oznamovat více zpracování, musí použít odpovídající počet formulářů. Úřad v tomto případě zastává názor, že každé zpracování je charakteristické především svým účelem a v případě, že by se v jednom formuláři objevovalo více účelů, mohlo by dojít k jejich smísení, což by způsobilo nejasnosti ohledně dalších informací obsažených ve formuláři. Využití tohoto formuláře však není zákonnou povinností oznamovatele, Úřad je proto povinen přijmout oznámení i ve formě standardního podání, tedy ve formě písemné, elektronické anebo ústní.[70]

Z odst. 3 §16 zákona o ochraně osobních údajů vyplývá oznamovateli právo předpokládat, že bylo jeho oznámení zpracováno a posouzeno jako vyhovující, tudíž může zpracování zahájit bez ohledu na to, jestli bylo jeho oznámení skutečně zaregistrováno. To platí v případě, že oznamovatel neobdrží od Úřadu do 30 dnů od doručení svého oznámení žádné, kladné ani záporné, odpovědi. Ve srovnání s jinými evropskými předpisy poskytuje zákon o ochraně

[70] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 249–251.

osobních údajů Úřadu na zpracování a posouzení oznámení poměrně krátkou dobu. Úřad musí oznámení nejprve formálně ověřit a zjistit, zda splňuje všechny zákonem stanovené náležitosti, zejména jestli obsahuje všechny informace požadované § 16 odst. 2 zákona o ochraně osobních údajů. Neobsahuje-li oznámení všechny formální náležitosti, vyzve Úřad oznamovatele k nápravě a určí mu k tomu přiměřenou lhůtu. Po opravě oznámení začíná Úřadu běžet nová 30-denní lhůta ke zpracování oznámení. Nedoplní-li oznamovatel požadované náležitosti ve stanovené lhůtě nebo nezareaguje vůbec na výzvu, bude na oznámení nahlíženo, jako by nikdy nebylo podáno, tudíž nedojde k jeho registraci a zamýšlené zpracování osobních údajů nesmí být zahájeno.

Je-li oznámení po formální stránce správné, je ověřen soulad s ostatními povinnostmi oznamovatele, jakožto budoucího správce osobních údajů, zejména ve smyslu povinností dle § 5 zákona o ochraně osobních údajů. Je-li oznámení Úřadem shledáno vyhovujícím po formální i věcné stránce, je přijato a zapsáno do veřejně dostupného registru oznámení. Shledá-li Úřad v doručeném oznámení rozpory s legalitou, zahájí s oznamovatelem řízení podle § 17 odst. 1 zmiňovaného zákona, jehož účelem je odstranění nejasností či problematických částí zamýšleného zpracování. Dojde-li k vyjasnění všech problémů, přistoupí Úřad k registraci. V případě, že by pochybnosti nebyly objasněny, vydá Úřad rozhodnutí o nepovolení oznámeného zpracování. Registrace oznámení je však prováděna pouze na základě předběžných informací, které jsou Úřadu sděleny oznamovatelem, došlo-li by následně již při samotném zpracování k odchýlení od zákonné úpravy, může Úřad provést kontrolní šetření a určit zpracovateli opatření k nápravě nebo příkaz k ukončení zpracování. Oznamovatel může Úřad požádat o vydání potvrzení, že došlo k registraci jeho zpracování. Toto osvědčení však prokazuje pouze skutečnost, že oznamovatel splnil svou zákonnou povinnost a také fakt, že jeho zpracování bylo registrováno. Registrační proces však nikdy nemůže z důvodů výše uvedených nahradit kontrolní řízení prováděné na místě, které má zjistit, zda je zpracování v souladu se zákonem. [71] Podle ustanovení § 16 odst. 6 zákona o ochraně osobních údajů neprovede Úřad registraci, je-li oznámení podané podle odst. 1 předmětem kontroly. Taková registrace může být provedena až po skončení kontroly s uspokojujícím výsledkem.[72]

[71] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 252–260.
[72] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář.* Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 254.

3. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Úřad pro ochranu osobních údajů (dále jen „Úřad“) je nezávislý orgán sídlící v Praze, který byl zřízen dne 1. 6. 2000 dle § 2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Až do účinnosti novely zákona č. 250/2014 Sb., o změně zákonů, souvisejících s přijetím zákona o státní službě, mu však byly kompetence ústředního správního orgánu pouze svěřeny, teprve od 1. 1. 2015 je považován za ústřední správní orgán pro oblast ochrany osobních údajů.

Úřad, jakožto dozorčí orgán v oblasti ochrany osobních údajů, byl zřízen na základě požadavku přímo vyplývajícího ze směrnice 95/46/ES. Tato směrnice i dodatek k Úmluvě č. 108 považují nezávislost Úřadu jako klíčový prvek ke splnění jeho základní funkce, kteroužto je ochrana osob v souvislosti se zpracováním osobních údajů. Nezávislost Úřadu, ať už po stránce organizační, právní, finanční či personální, je zajištěna v části první Hlavě IV. a V. zákona o ochraně osobních údajů. Úřad se dle těchto ustanovení řídí zákony a jinými právními předpisy, ve své činnosti je nezávislý a do jeho pravomocí lze zasahovat jen na základě zákona. Právními předpisy nižší právní síly se řídí jen v případech činností, které nespadají do jeho pravomoci, například v případě jeho hospodaření se svěřeným majetkem.

Úřad pro ochranu osobních údajů nespadá do hierarchie státní správy řízené vládou. Není odpovědný vládě, ministerstvu ani žádnému jinému orgánu, čímž se podobá Českému telekomunikačnímu úřadu, Energetickému regulačnímu úřadu nebo Radě pro rozhlasové a televizní vysílání.[73] Vláda i ministerstva a jim podřízené orgány, zastávají pozici správce a zpracovatele osobních údajů, proto je nezávislost Úřadu tak důležitá. Nezávislost Úřadu však nelze srovnávat s nezávislostí soudů, protože stále zůstává správním úřadem.

Důležité je také to, že Úřad má svou vlastní kapitolu ve státním rozpočtu ČR, ze které je hrazena jeho činnost, což rovněž přispívá k jeho nezávislosti, přičemž předseda Úřadu má právo účastnit se jednání rozpočtového výboru Poslanecké sněmovny Parlamentu České republiky.

Dalším prvkem nezávislosti je personální složení Úřadu, které tvoří předseda, inspektoři a další zaměstnanci. Kontrolní činnost Úřadu je prováděna

[73] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 305.

inspektory a pověřenými zaměstnanci, na základě kontrolního plánu nebo na základě podnětů a stížností. Předseda stojí v čele Úřadu, je jmenován a odvoláván prezidentem ČR na návrh Senátu Parlamentu ČR. Jeho funkční období je 5 let a může být jmenován maximálně na dvě po sobě jdoucí období, musí být občanem ČR. Inspektor je taktéž jmenován a odvoláván prezidentem ČR na návrh Senátu Parlamentu ČR. Jeho volební období je 10 let a může být jmenován i opakovaně. Důležitá je pak neslučitelnost funkcí předsedy Úřadu i inspektora s funkcí senátora, poslance, soudce, státního zástupce, s jakoukoli funkcí ve veřejné správě či člena orgánu územní samosprávy a s jejich členstvím v politických stranách a hnutích.[74] Podle ustanovení § 30 odst. 3 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, se *„na zaměstnance Úřadu vztahují ustanovení zákoníku práce, pokud tento zákon nestanoví jinak“*. Zákoník práce se pak nevztahuje na některé otázky pracovního poměru předsedy Úřadu a inspektorů, konkrétně na jejich platové poměry a na způsob jejich jmenování a odvolání. Další specifikace je obsažena v § 30 odst. 4 a 5, § 32 a § 33 zákona o ochraně osobních údajů.[75]

Působnost Úřadu je stanovena § 2 a § 29 tohoto zákona, a v případě zvláštních agend zvláštními právními předpisy, popř. přímo použitelnými předpisy EU a mezinárodními smlouvami, jež jsou součástí našeho právního řádu. Jeho činnost spočívá zejména v provádění dozoru nad dodržováním zákonem stanovených povinností při zpracování osobních údajů, vedení registru zpracování osobních údajů, přijímání podnětů a stížností občanů na porušení zákona a v poskytování konzultace v oblasti ochrany osobních údajů.[76] K povinnostem Úřadu patří také zpracování výroční zprávy, která vypovídá o jeho činnosti a její následné zveřejnění. Výroční zpráva informuje zejména o provedené kontrolní činnosti a její zhodnocení, shrnuje informace a hodnotí stav v oblasti zpracování a ochrany osobních údajů v České republice i ostatní činnosti Úřadu.

Úřad projednává, na základě § 29 odst. 1 písm. e) zákona o ochraně osobních údajů, správní delikty a ukládá za ně nápravná opatření a sankce nejen dle zákona na ochranu osobních údajů, ale také podle dalších právních předpisů, např. dle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (§ 17e), dále dle zákona č. 328/1999 Sb., o občanských

[74] § 32 a § 34 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[75] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 320.
[76] § 29 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

průkazech (§ 16a–c) a dle zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky (§ 34a–c).

Ve své správní činnosti postupuje Úřad dle speciálních ustanovení obsažených v zákoně o ochraně osobních údajů a podle obecného právního předpisu, kterým je zákon č. 500/2004 Sb., správní řád. V případě své dozorovací činnosti se Úřad řídí zákonem č. 255/2012 Sb., o kontrole, dále pak § 37 a § 40 zákona o ochraně osobních údajů. Dozor a kontrola jsou zde chápány jako dva odlišné pojmy. Kontrola je pojem užší, přičemž je prováděna jen v rámci specifického časového úseku, oproti tomu dozor je chápán jako činnost Úřadu, která je vykonávána soustavně.[77]

Ministerstvo vnitra a Policie ČR jsou povinni spolupracovat s Úřadem pro ochranu osobních údajů a poskytnout mu referenční údaje ze základního registru obyvatel a údaje z agendového informačního systému evidence obyvatel a cizinců.[78] Údaji z těchto evidencí jsou např. jméno, příjmení a adresa pobytu, ty však lze poskytnout jen v případě, kdy je to nezbytně nutné ke splnění daného úkolu. Tento předpoklad nezbytné nutnosti ilustruje skutečnost, že i Úřad pro ochranu osobních údajů se musí řídit zásadou vázanosti účelem zpracování osobních údajů, která ukládá povinnost zpracovávat osobní údaje jen v souladu s účelem, k němuž byly shromážděny a jejich zpracování k jinému účelu je vázané na souhlas subjektu údajů, nebo na případy stanovené v § 3 odst. 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.[79]

Úřad taktéž podléhá povinnosti poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, které se vztahují k jeho působnosti.

3.1 Pravomoci a postavení podle GDPR

V souvislosti s přijetím obecného 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále také pod zkratkou „GDPR“, tedy General Data Protection Regulation) stále platí, že Úřad

[77] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5, s. 314.
[78] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0, s. 322.
[79] § 29a zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

je nadále ústředním správním orgánem pro oblast ochrany osobních údajů. Mezi jeho hlavní úkoly však nově patří také monitorování a vymáhání uplatňování práv a povinností dle obecného nařízení a dalších předpisů, které upravují některé otázky ochrany osobních údajů. K jeho povinnostem patří také osvětová a konzultační činnost, při níž poskytuje poradenství např. Parlamentu ČR, vládě a dalším orgánům a institucím, zejména pak v souvislosti s jejich legislativní činností. Do jeho působnosti spadá problematika ochrany osobních údajů, na kterou se výše zmíněné obecné nařízení nevztahuje, zároveň je z jeho působnosti vyňato takové zpracování osobních údajů, které je prováděno určenými skupinami správců.[80]

Na základě čl. 51 GDPR a v souvislosti s ustanovením § 2 zákona o ochraně osobních údajů, je dozorová činnost pro oblast ochrany osobních údajů pravomocí Úřadu na ochranu osobních údajů. Ten zastává funkci ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu, který je stanoven tímto nařízením, zákonem o ochraně osobních údajů, zvláštními právními předpisy a mezinárodními smlouvami, jež jsou součástí našeho právního řádu. Přestože čl. 51 odst. 1 GDPR říká, že: *„každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování tohoto nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie.“*, je Úřad jediným dozorovým úřadem s obecnou působností v ČR.

Článek 52 GDPR pak výslovně požaduje nezávislost samotného dozorového úřadu i jeho členů, přičemž jejich činnost nesmí být nijak ovlivňována, ať už přímo nebo nepřímo. Zároveň také nesmí od nikoho mimo Úřad dostávat ani přijímat pokyny k plnění jejich povinností. Je zde zřejmá neslučitelnost funkcí členů v průběhu funkčního období, která je specifikována v § 32 a § 34 zákona o ochraně osobních údajů. Článek 53 GDPR stanovuje požadavek na jmenování členů Úřadu, jež souhlasí s podmínkami jmenování v naší vnitrostátní úpravě. Znění čl. 54 odst. 2 GDPR stanovuje povinnost mlčenlivosti pro všechny členy a pracovníky Úřadu po dobu trvání jejich funkčního období, ale i po jeho skončení. V čl. 55 odst. 3 GDPR potvrzuje nezávislost soudní moci tím, že shledává dozorové úřady nepříslušné k dozoru

[80] Dozorová činnost. *Uoou.cz* [online]. [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/rd=0

nad operacemi zpracování, které provádějí soudy jednající v rámci svých soudních pravomocí.

Věcná působnost Úřadu v oblasti dozoru spočívá především v činnostech podle ustanovení čl. 57 odst. 1 písm. a), f), h). Úřad tedy monitoruje a vymáhá uplatňování tohoto nařízení, zabývá se stížnostmi subjektů údajů, prošetřuje předmět obdržené stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření a provádí šetření o uplatňování nařízení zejména na základě informací obdržených od jiného orgánu veřejné moci.[81]

Úřad je podle čl. 58 odst. 2 GDPR oprávněn upozornit správce či zpracovatele, že zpracováním porušují nařízení, udělit správci či zpracovateli napomenutí, nařídit správci a zpracovateli, aby vyhověli žádosti subjektu údajů výkon jeho práv, nařídit soulad zpracování osobních údajů s tímto nařízením, také nařídit, aby byl subjekt údajů informován o porušení zabezpečení osobních údajů, uložit dočasné nebo trvalé omezení zpracování včetně zákazu, nařídit opravu či výmaz osobních údajů nebo omezení zpracování, odebrat osvědčení nebo zamezit jeho vydání, zakázat předání osobních údajů příjemci, anebo uložit správní pokutu vedle či namísto výše uvedených opatření podle článku 83 tohoto nařízení. Její výše pak závisí na tom, jaké ustanovení bylo porušeno. Správní pokuta musí být ukládána přiměřeně, s ohledem na účinnost a tak, aby měla odrazující charakter. Prakticky nikdo tak neobdrží pokutu při horní hranici. Aby se tak stalo, muselo by dojít k několika velmi závažným porušením zároveň. Došlo-li tedy například k porušení povinnosti zabezpečit osobní údaje podle čl. 32 GDPR, je za toto porušení možné udělit pokutu až do výše 10 mil. EUR, v případě podniku pokutu do výše 2 % jeho celkového celosvětového ročního obratu za předchozí finanční rok, dle toho, která hodnota je vyšší. Pokud byly porušeny základní zásady pro zpracování a podmínky udělení souhlasu (čl. 5, 6, 7 a 9 GDPR) nebo práva subjektů (čl. 12 až 22 GDPR) lze uložit správní pokutu do výše 20 mil. EUR a v případě podniku až do výše 4 % jeho celkového celosvětového ročního obratu za předchozí finanční rok, opět dle toho, která hodnota je vyšší. Členské státy pak mají právo stanovit pravidla pro ukládání sankcí za porušení tohoto nařízení, zejména za porušení, na které se nevztahují správní pokuty podle čl. 83 GDPR a učinit veškerá opatření pro zajištění jejich uplatňování. Jde například o sankce podle § 44 zákona o ochraně osobních údajů.

[81] 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Ukládání těchto sankcí musí být v souladu se zásadou ne bis in idem. Členský stát, který se rozhodl tyto odlišné sankce přijmout, musel tento úmysl oznámit do 25. května 2018 Evropské komisi.[82]

[82] NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 513–527.

4. GDPR

Vzhledem k neustále rostoucímu vývoji nových technologií, potřebě zajistit nová technická a organizační opatření k ochraně osobních údajů a nedostatku personálního obsazení, které by fungování této ochrany zajistilo, se ukázala být dosavadní směrnice 95/46/ES do budoucna již nedostačující. Právě proto došlo k přijetí nového obecného nařízení známého spíše pod názvem GDPR, tzn. General Data Protection Regulation. Jelikož bylo GDPR přijato jako nařízení a nikoli směrnice, stalo se datem své účinnosti, tedy dnem 25. května 2018, přímo aplikovatelným bez nutnosti implementace do vnitrostátního práva členských států, kterou by směrnice vyžadovala. Toto nařízení tedy přímo určuje pravidla pro zpracování osobních údajů ve všech zemích EU i práva subjektů, jimiž jsou výhradně fyzické osoby po dobu svého života. GDPR je tedy univerzálně použitelné ve všech členských státech EU, zároveň tak mimo jiné dochází ke sjednocení úpravy ochrany osobních údajů ve všech členských státech. V ČR GDPR částečně nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, přičemž by měl být vydán zákon nový, který by se omezil jen na některé otázky zpracování osobních údajů, které GDPR nezachycuje a tam, kde mu to GDPR dovolí, stanovit některé odchylky, například výši pokut za porušení předpisů o ochraně osobních údajů aj. Nově vzniklý zákon o zpracování osobních údajů by měl obsahovat i úpravu postavení a organizace Úřadu pro ochranu osobních údajů.

Cílem GDPR je tedy sjednocení právní regulace v oblasti ochrany osobních údajů a zajištění, aby byla tato regulace v souladu s dnešními technologickými poznatky. Dále chce také posílit práva subjektů údajů a docílit svého jednotného výkladu prostřednictvím dozorových úřadů jednotlivých členských zemí. Důvodem jeho přijetí byla také reakce na rozvíjející se obchodní styky se státy mimo EU, kdy jednotnost systému ošetřujícího tuto důležitou problematiku posiluje důvěryhodnost Evropské unie jako obchodního partnera.

Jelikož přijetí GDPR přináší značné změny v oblasti ochrany osobních údajů a jejich zpracování, byla stanovena poměrně dlouhá legisvakanční lhůta, tedy zatímco platnost nastala 27. dubna 2016, jeho účinnost byla odložena až na 25. května 2018. Teprve od termínu účinnosti se GDPR stává plně použitelným a vymahatelným pro oblast ochrany osobních údajů. Tímto nařízením se tedy budou řídit správci, zpracovatelé, příslušné orgány státní

správy, především pak Úřad pro ochranu osobních údajů, a jiné úřady. Ochranu osobních údajů podle § 316 zákoníku práce řeší Státní úřad inspekce práce a jednotlivé inspektoráty práce. GDPR se naopak nevztahuje na zpracování osobních údajů pro osobní či domácí činnost a neupravuje ani zpracování osobních údajů prováděné příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestních činů nebo výkonu trestů, tato problematika je předmětem úpravy směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Vzhledem k tomu, že se jedná o směrnici, není možné ji použít přímo, a proto bude nutná její implementace do českého právního řádu, kupříkladu prostřednictvím zákona č. 273/2008 Sb., o Policii České republiky, nového zákona o zpracování osobních údajů či a jiných právních předpisů.

Toto nařízení do problematiky vnáší mnoho změn i nových prvků, zakotvuje nová práva subjektů údajů i nové povinnosti správců. Obecně je GDPR založeno na dvou nových přístupech, přístupu odpovědnosti a přístupu založeném na riziku. Princip odpovědnosti reflektuje odpovědnost správce za dodržování zásad zpracování, které jsou uvedeny v ustanovení čl. 5 odst. 1 GDPR, přičemž má zároveň povinnost jejich dodržování doložit, k čemuž může sloužit například osvědčení či certifikace příp. záznamy o činnostech zpracování.[83] Princip založený na riziku vyjadřuje povinnost správce již od počátku zpracování osobních údajů brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob, čemuž musí přizpůsobit i zabezpečení osobních údajů a procesu jejich zpracování. Jedná se tedy o uložení některých povinností v situaci, kdy zpracování osobních údajů či porušení zabezpečení představuje riziko pro práva a svobody fyzické osoby. Jedná se zejména o povinnost ohlašovací v případě porušení bezpečnosti, o posuzování vlivu zpracování na ochranu osobních údajů aj.[84]

[83] NAVRÁTIL, Jiří. *GDPR pro praxi.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 28–32.
[84] Sdělení ÚOOÚ k přístupu založenému na riziku. *Uoou.cz* [online]. 2016 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=26872

4.1 Zásady zpracování osobních údajů

Základní zásady zpracování osobních údajů jsou vymezeny v ustanovení článku 5 GDPR. Jedná se o základní pravidla, jimiž se musejí řídit všichni správci při zpracování osobních údajů, přičemž musí nově soulad s nimi prokazovat. Pro dodržení této povinnosti bude muset správce uchovávat všechny důkazy týkající se všech opatření, která přijal s úmyslem zajistit soulad s tímto nařízením. Základní zásady však nejsou v evropském právním rámci ochrany údajů žádnou novinkou.

4.1.1 Zásada zákonnosti

Tato základní a pravděpodobně i nejdůležitější zásada ochrany osobních údajů stanoví, že zpracování osobních údajů je možné jen na základě jednoho z právních titulů definovaných v čl. 6 odst. 1 GDPR a zároveň nesmí být v rozporu se zákonem. Zpracování jedné kategorie osobních údajů může být ve stejnou dobu realizováno i pro více účelů. Nesmí však směřovat za nelegálním či nelegitimním účelem. Zpracování tudíž musí být v souladu s GDPR i s právním řádem obecně. Za porušení této zásady můžeme považovat zejména zpracování osobních údajů bez právního titulu podle čl. 6 nebo zpracování citlivých údajů bez naplnění některé z výjimek podle čl. 9 GDPR.

4.1.2 Zásada korektnosti a transparentnosti

Tyto zásady ukládají správci povinnost zpracovávat osobní údaje otevřeně a zajistit, aby byl subjekt údajů o tomto zpracování vhodně informován. Nejvíce se promítají v informační povinnosti podle čl. 13 a čl. 14 GDPR, jejíž porušení je nejčastějším případem nedodržení těchto zásad. K jejich porušení dojde také v případě odepření práva subjektu údajů na přístup k osobním údajům podle čl. 15 tohoto nařízení. Projevem transparentnosti může být také informování dozorčího úřadu o závažných porušeních zabezpečení osobních údajů podle čl. 34 nařízení.

4.1.3 Zásada účelového omezení

Tato zásada správci zakazuje zpracovávat osobní údaje pro jiné účely, než pro které byly shromážděny, až na výjimky podle čl. 5 odst. 1 písm. b) a čl. 6 odst. 4 GDPR. Ty jsou pouze 4, konkrétně zpracování pro účely archivace

ve veřejném zájmu, pro účely historického výzkumu či pro statistické účely, jež je v souladu s čl. 89 odst. 1 GDPR, zpracování se souhlasem subjektu údajů, je-li zpracování v souladu s právem členského státu nebo je-li původní účel slučitelný s účelem následným podle čl. 6 odst. 4 GDPR. Určení účelu je významné také pro aplikovatelnost dalších zásad.

4.1.4 Zásada minimalizace údajů a zásada přesnosti

Podle zásady minimality může správce zpracovávat jen ty osobní údaje, jejichž zpracování je pro dosažení předem stanoveného účelu relevantní a nezbytné. Zásadou přesnosti je pak vysloven předpoklad, že všechny zpracovávané osobní údaje jsou přesné, odpovídají skutečnosti a v případě nutnosti je možná jejich aktualizace. Nebyly-li by údaje přesné, pak musí správce jejich nepřesnost opravit, popř. je zlikvidovat.

4.1.5 Zásada omezení uložení

Zakotvuje povinnost správce vymazat nebo anonymizovat ty osobní údaje, které již nejsou pro naplnění stanoveného účelu potřebné. Jinak řečeno, tato zásada vystihuje povinnost správce uchovávat osobní údaje jen po dobu, po kterou je to pro naplnění stanoveného účelu nezbytně nutné. Dojde-li však k anonymizaci údajů, resp. k zamezení schopnosti přiřadit osobní údaje ke konkrétní fyzické osobě, nespadají tyto nadále do působnosti GDPR ani zákona o ochraně osobních údajů, protože anonymizované údaje se již za osobní údaje nepovažují.

4.1.6 Zásada integrity a důvěrnosti

Na základě těchto zásad je správce povinen přijmout taková technická a organizační opatření, aby zabránil nejen neoprávněnému či protiprávnímu zpracování osobních údajů, ale i jejich nahodilé ztrátě, zničení nebo poškození. Konkrétní požadavky na zabezpečení osobních údajů jsou stanoveny v čl. 32 GDPR.

4.1.7 Zásada odpovědnosti

Tato zásada nakonec ukládá správci povinnost zajistit soulad se všemi výše uvedenými zásadami a zároveň povinnost být schopen tento soulad prokázat. Nutnost prokázání souladu je novinkou. Pro dodržení této povinnosti bude muset

správce uchovávat důkazy týkající se všech opatření, která přijal, aby soulad s tímto nařízením zajistil. Zásada je blíže rozvedena v ustanovení čl. 24 daného nařízení.[85]

4.2 Souhlas se zpracováním

Právní úprava souhlasu obsažená v GDPR jeho parametry v zásadě nemění, ale požadavky na něj rozšiřuje. Nová definice souhlasu je uvedena v čl. 4 odst. 11 tohoto nařízení a říká, že: *„souhlas subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*. Ani GDPR nepožaduje, aby byl souhlas písemný. Uvádí však, že nečinnost ani předem zaškrtnutá políčka by neměla být za souhlas považována. Nařízení stejně jako zákon o ochraně osobních údajů požaduje, aby byl správce, resp. zpracovatel schopný doložit existenci souhlasu.

GDPR ve svém čl. 7 odst. 2 říká, že: „*pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.*“ Zde je tedy kladen důraz především na srozumitelnost a dobrovolnost daného souhlasu.

Tato právní úprava vylučuje další existenci případů, kdy správci zahrnují souhlas se zpracováním do smluvního ujednání, od kterého se nemůže fyzická osoba odchýlit, nejčastějším takovým případem je přítomnost souhlasu v obchodních podmínkách. Lze tedy s určitostí říci, že souhlas se zpracováním osobních údajů již nemůže být považován za nezbytnou podmínku poskytnutí služby či koupě zboží. V souladu s ustanovením čl. 7 odst. 4 GDPR, které říká, že: *„Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.“* by taková forma udělení souhlasu byla považována za neplatnou. Souhlas se zpracováním musí být uveden mimo smluvní ujednání, musí být srozumitelný, získán transparentním způsobem a musí být udělen dobrovolně. Za neplatný

[85] NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7, s. 105–123.

by byl zajisté považován takový souhlas, kdy by byl zákazník nucen při získání služby nebo výrobku souhlasit zároveň se zpracováním osobních údajů. Toto obecné nařízení v ustanovení čl. 7 odst. 3 také nově zakotvuje právo subjektu souhlas se zpracováním kdykoli odvolat, přičemž zároveň říká, že: *„Odvolat souhlas musí být stejně snadné jako jej poskytnout.“* Tato úprava se až do okamžiku přijetí GDPR v českém právu nevyskytovala a možnost souhlas odvolat se pouze dovozovala z ustanovení směrnice 95/46/ES. Obecně platí, že došlo-li subjektem údajů k odvolání souhlasu se zpracováním, pak veškeré operace, které proběhly před jeho odvoláním, zůstávají zákonné, přesto však musí správce neprodleně veškerou další zpracovatelskou činnost, které se odvolání souhlasu týkalo, zastavit.[86] Zpracování osobních údajů by mělo být legální i bez souhlasu subjektu údajů, pokud je zpracování nezbytné pro ochranu života a zdraví subjektu či životně důležitého zájmu jiných fyzických osob, jako např. epidemie, živelná pohroma apod. Mezi oprávněné zájmy správce podle GDPR patří jak zpracování osobních údajů, které má zamezit podvodům, čímž v podstatě dochází k legalizaci databází dlužníků a neplatičů, jejichž provozování bylo doteď problematické, tak i zpracování pro účely přímého marketingu.

4.3 Právo na námitku

Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést proti zpracování osobních údajů, které se jej týkají, na základě čl. 6 odst. 1 písm. e)[87] nebo f)[88] GDPR, námitku, a to i v případech profilování[89]. Správce pak nadále nesmí osobní údaje zpracovávat, jestliže neprokáže závažné a oprávněné důvody pro jejich zpracování.[90]

Dochází-li ke zpracování osobních údajů pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů,

[86] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1, s. 11–15.
[87] Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.
[88] Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.
[89] Profilování je 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 – článek 4 odst. 4 GDPR.
[90] Ust. čl. 21 odst. 1 GDPR.

které se ho týkají, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu. Pokud subjekt údajů vznese proti tomuto zpracování námitku, nebudou již osobní údaje pro tyto účely zpracovávány.[91]

Subjekt údajů musí být o tomto právu řádně informován nejpozději v okamžiku první komunikace se správcem, a to způsobem, který toto právo zřetelně a jasně oddělí od ostatních informací.

4.4 Právo na přenositelnost osobních údajů

Subjekt údajů má právo získat od správce osobní údaje jím poskytnuté a předat je správci jinému, aniž by tomu mohl původní správce bránit, v případě, že ke zpracování osobních údajů dochází na základě souhlasu nebo smlouvy, nebo v případě, kdy je zpracování prováděno automatizovaně. Subjekt má také právo na to, aby byly zpracovávané údaje jedním správcem předány správci druhému přímo, je-li to technicky proveditelné. Na toto právo musí být subjekt údajů taktéž upozorněn a to stejně, jako je tomu v případě práva na podání námitky.

Toto právo se však neuplatní v případě zpracování, které je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen. Právem na přenositelnost nesmí být nijak dotčena práva a svobody jiných osob.

4.5 „Právo být zapomenut“

Právo na výmaz není absolutním právem. Je možné jej uplatnit pouze ve chvíli, kdy již nejsou osobní údaje potřebné pro účel, pro který byly shromážděny nebo zpracovávány. Toto právo je upraveno v ustanovení čl. 17 GDPR, přičemž podle něj má subjekt údajů právo, aby správce bez zbytečného odkladu vymazal osobní údaje subjektu tehdy, je-li splněn alespoň jeden z následujících důvodů:

1) osobní údaje již nejsou nadále potřebné pro původní účely zpracování,
2) subjekt údajů odvolá souhlas se zpracováním údajů a pro jejich další zpracování neexistuje právní důvod,
3) subjekt údajů vznesl proti zpracování námitky a po zpracování není jiný oprávněný důvod,
4) k zpracování osobních údajů došlo protiprávně,

[91] Ust. čl. 21 odst. 2 a 3 GDPR.

5) vymazání osobních údajů rozhodl příslušný orgán,
6) došlo-li ke shromáždění osobních údajů v souvislosti s nabídkou zboží či služeb.[92]

Jestliže by tedy správce mezitím osobní údaje zveřejnil nebo předal, je povinen přijmout příslušné kroky k jejich vymazání. V případě, že by došlo k předání osobních údajů na více míst, může se zajištění jejich vymazání stát velmi nákladným.

Z povinnosti výmazu existuje také několik výjimek, při jejichž existenci nemusí k výmazu dojít. Jde o případy, u nichž je zpracování nezbytné:

1) pro výkon práva na svobodu projevu a informace,
2) pro splnění právní povinnosti,
3) z důvodu veřejného zájmu v oblasti veřejného zdraví,
4) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,
5) pro určení, výkon nebo obhajobu právních nároků.[93]

4.6 Posouzení dopadu činnosti na ochranu osobních údajů

Povinnost provést posouzení vlivu je upraveno článkem 35 GDPR, který říká: „*pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů*.“ Toto posouzení nahradilo obecnou ohlašovací povinnost zpracování osobních údajů Úřadu zakotvenou ve směrnici 95/46/ES.

Posouzení vlivu by mělo být vypracováno v případech, kdy dochází k rozsáhlým operacím zpracování na regionální, celostátní či nadnárodní úrovni, přičemž takovéto zpracování by mělo vliv na velký počet subjektů údajů a rovněž by s sebou neslo i vysoké riziko.[94] Dále by k posouzení vlivu mělo dojít v případě značně rozsáhlého použití nové technologie nebo v případech, kdy dochází ke zpracování citlivých údajů podle článku 9 odst. 1 nebo zpracování osobních údajů týkajících se rozsudků v trestních věcech podle článku 10 GDPR. V případě

[92] Ust. čl. 17 odst. 1 písm. a) až f) GDPR.
[93] Ust. čl. 17 odst. 3 písm. a) až e) GDPR.
[94] Recitál 91 GDPR.

rozsáhlého monitorování veřejných prostor je posouzení vlivu na ochranu osobních údajů taktéž zapotřebí realizovat. Posouzení vlivu však není vázáno jen na zákonem vymezené důvody. Toto posouzení se může stát užitečným například u společností s alespoň 250 zaměstnanci, jeho užití totiž může předejít vzniku zásadnějších problémů s ochranou osobních údajů.[95]

Vyplývá-li z posouzení vlivů, že by zpracování osobních údajů mělo za následek vysoké riziko pro práva a svobody fyzických osob, je správce a zpracovatel povinen svůj úmysl zpracovávat osobní údaje konzultovat s Úřadem pro ochranu osobních údajů, a to ještě před samotným započetím zpracování.[96]

Byl-li jmenován pověřenec pro ochranu osobních údajů, vyžádá si správce při provádění posouzení vlivu jeho posudek. Posouzení vlivů by podle ustanovení článku 35 odst. 7 GDPR mělo přinejmenším obsahovat systematický popis zamýšlených operací zpracování osobních údajů a účely zpracování, popř. oprávněné zájmy správce, dále pak posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů, posouzení rizik pro práva a svobody subjektů údajů a plánovaná opatření k řešení těchto rizik, včetně záruk a bezpečnostních opatření k zajištění ochrany osobních údajů a k doložení souladu s GDPR, s přihlédnutím k oprávněným zájmům subjektů údajů a dalších dotčených osob. Správce by měl vyhodnotit zejména původ, povahu, zvláštnost a závažnost případného rizika. Výsledek posouzení by pak měl být zohledněn při rozhodování o přijetí příslušných opatření, která by měla prokázat soulad zpracování s GDPR.[97]

4.7 Konzultace s Úřadem pro ochranu osobních údajů

Nařízení nově definuje povinnost správce provádět konzultace s Úřadem pro ochranu osobních údajů, přičemž ta má nahradit dřívější registrační povinnost. Nelze však teď ani do budoucna předpokládat, že tyto konzultace budou obdobou bezplatné právní poradny zejména z důvodu nedostatečného personálního vybavení Úřadu. Bude se však jednat o prostředek, jehož pomocí bude možné zamezit mnohým chybám, ke kterým při zpracování osobních údajů dochází. Avšak odpovědnost za zpracování bude stále dopadat na správce a zpracovatele.

Tato nová povinnost je vymezena v článku 36 GDPR, ten říká, že k takové konzultaci musí dojít ještě před samotným zpracováním osobních údajů,

[95] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 81–83 a 102.
[96] Recitál 94 GDPR.
[97] Recitál 84 GDPR.

pokud z posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR vyplývá, že by dané zpracování s sebou mohlo nést vysoké riziko narušení ochrany osobních údajů, pokud by správce nepřijal opatření k jeho zmírnění.[98] Při této konzultaci musí správce Úřadu poskytnout informace o rozdělení odpovědnosti mezi správci nebo zpracovateli, informace o účelu a způsobu zamýšleného zpracování, o realizovatelných opatřeních a zárukách pro ochranu základních práv a svobod subjektů údajů, kontaktní údaje případného pověřence, posouzení vlivu podle čl. 35 GDPR a veškeré další informace, o které Úřad oprávněně požádá.[99]

Dojde-li Úřad k názoru, že by případné zpracování porušilo ustanovení GDPR, popř. jiný relevantní právní předpis, informuje o tom správce, resp. zpracovatele písemně nejpozději do 8 týdnů od obdržení žádosti o konzultaci. Tuto lhůtu lze až o 6 týdnů prodloužit s ohledem na složitost zamýšleného zpracování. O případném prodloužení a jeho důvodech však musí dozorový úřad správce či zpracovatele vyrozumět nejpozději do jednoho měsíce od obdržení žádosti o konzultaci. Tyto lhůty mohou být pozastaveny až do doby, kdy Úřad obdrží veškeré informace, které si pro účely konzultace vyžádal.[100]

V případě, že Úřad v rámci předběžné konzultace dojde k názoru, že správce, resp. zpracovatel nedostatečně určil či zmírnil riziko zpracování, může:

1) správci a zpracovateli nařídit, aby mu poskytli veškeré informace, které k naplnění svých úkolů potřebuje,
2) zahájit šetření formou auditu ochrany údajů s cílem zjistit potřebné informace, a potom přistoupit k dalším opatřením,
3) přezkoumat všechna osvědčení, která byla správci a zpracovateli vydána na základě čl. 42 GDPR a případně je odebrat,
4) ohlásit správci a zpracovateli porušení ustanovení GDPR, což pravděpodobně způsobí zahájení správního řízení o uložení pokuty či jiné sankce,
5) si od správce a zpracovatele vyžádat přístup k veškerým informacím, které potřebuje k výkonu svých úkolů,

[98] Ust. čl. 36 odst. 1 GDPR.
[99] Ust. čl. 36 odst. 3 písm. a) až f) GDPR.
[100] Ust. čl. 36 odst. 2 GDPR.

6) si vyžádat přístup do všech prostor, kde správce a zpracovatel působí, popř. přístup k veškerému zařízení a prostředkům určeným ke zpracování údajů.[101]

4.8 Vedení záznamů o zpracovávání osobních údajů

Každý správce a jeho případný zástupce jsou povinni vést záznamy o činnostech zpracování, za něž správce odpovídá. Tyto záznamy musí obsahovat alespoň:

1) jméno a kontaktní údaje správce, případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,
2) účely zpracování,
3) popis kategorií subjektů údajů a kategorií osobních údajů,
4) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
5) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace,
6) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů,
7) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.[102]

Zpracovatel má stanovenou odlišnou strukturu v ustanovení článku 30 odst. 2 GDPR.

Tyto záznamy musí být vedeny v písemné, resp. elektronické formě a musí být na vyžádání Úřadu pro ochranu osobních údajů předloženy.[103] Výjimku z vedení těchto záznamů mají podniky nebo organizace zaměstnávající méně než 250 osob, ledaže by zpracování osobních údajů jimi prováděné představovalo riziko pro práva a povinnosti subjektů údajů, nedochází-li ke zpracování příležitostně nebo zahrnuje-li zpracování zvláštní kategorie osobních údajů podle čl. 9, popř. osobní údaje týkající se rozsudků v trestních věcech podle

[101] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 125–126.
[102] Ust. čl. 30 odst. 1 písm. a) až g) GDPR.
[103] Ust. čl. 30 odst. 3 a 4 GDPR.

čl. 10 GDPR.[104] I zde platí povinnost správce doložit zabezpečení souladu s GDPR a případné spolupráce s dozorovým úřadem.[105]

4.9 Zabezpečení osobních údajů a hlášení narušení bezpečnosti

Povinnost správce zabezpečit osobní údaje vyplývá ze zásady integrity, důvěrnosti a ze zásady odpovědnosti. Podle nich musí ke zpracování osobních údajů docházet pouze takovým způsobem, který zajistí jejich zabezpečení a zároveň je ochrání před nelegitimním a nelegálním zpracováním, popř. před jejich ztrátou, zničením nebo poškozením. Správce je taktéž povinen pro řádné zabezpečení přijmout přiměřená opatření, přičemž jejich přijetí musí být schopen doložit.

Zabezpečení osobních údajů je upraveno článkem 32 GDPR, který říká, že: „*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, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně pseudonymizace a šifrování osobních údajů, schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů, procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*“ Za porušení zabezpečení osobních údajů je považováno takové porušení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí, popř. zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.[106]

GDPR přináší ve svých článcích 33 a 34 úplnou novinku v podobě ohlašování bezpečnostních incidentů. Jedná se o povinnost správce ohlašovat případy porušení zabezpečení osobních údajů jednak příslušnému dozorovému úřadu, v tomto případě Úřadu pro ochranu osobních údajů, ale také subjektu údajů bez zbytečného odkladu a, je-li to možné, nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvěděl, a to tehdy, je-li pravděpodobné,

[104] Ust. čl. 30 odst. 5 GDPR.
[105] Recitál 82 GDPR.
[106] Ust. čl. 32 odst. 2 GDPR – pozitivní definice, nutno ji negovat.

že porušením došlo k ohrožení práv a svobod fyzických osob. Není-li možné poskytnout vše požadované současně, je nutno je bez zbytečného odkladu doplnit ihned, jakmile to bude možné. Dojde-li k nedodržení zákonem stanovené lhůty, musí správce objektivní důvody jejího nedodržení doložit.[107]

V případě, že by porušení zabezpečení zjistil zpracovatel, oznámil by tuto skutečnost neprodleně správci, ten by pak postupoval dle výše stanoveného postupu.[108] Ohlášení by mělo obsahovat minimálně popis daného porušení zabezpečení včetně kategorií ohrožených údajů včetně jejich subjektů, kontaktní údaje pověřence, popis pravděpodobných důsledků porušení zabezpečení a popis opatření, která správce přijal pro vyřešení nebo zmírnění následků tohoto porušení.

V případě, kdy porušení zabezpečení může mít za následek velké riziko ohrožení práv a svobod fyzických osob, je správce povinen tento bezpečnostní incident oznámit kromě Úřadu pro ochranu osobních údajů také přímo subjektu údajů.[109] Toto oznámení pak musí obsahovat alespoň kontaktní údaje pověřence, možné důsledky porušení zabezpečení a popis opatření, jež správce přijal pro vyřešení, popř. zmírnění vzniklé situace.[110] Oznámení subjektu údajů nemusí správce provést v případě, kdy došlo k porušení zabezpečení nesrozumitelných nebo zašifrovaných údajů, přijal-li správce opatření zamezující vzniku vysokého rizika pro práva a svobody fyzických osob, nebo v případě, kdy by bylo pro informování subjektů údajů ze strany správce nutné vynaložit nepřiměřené úsilí, v takovém případě by však správce musel využít veřejného nebo obdobného oznámení.[111]

Při určování možného rizika bude vždy nutné zohlednit kategorii údajů, jejíž zabezpečení bylo porušeno, přičemž vyššímu riziku budou logicky podléhat zvláštní kategorie údajů podle článku 9 GDPR.

4.10 Pověřenec pro ochranu osobních údajů

Definice pověřenec pro ochranu osobních údajů (dále jen „pověřenec“), jeho jmenování, postavení a úkoly jsou upravené v článcích 37 až 39 GDPR. Pověřenci plní funkci expertů v oblasti ochrany osobních údajů, přičemž mají

[107] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 129.
[108] Ust. čl. 33 odst. 1 a 2 GDPR.
[109] Ust. čl. 34 odst. 1 GDPR.
[110] Ust. čl. 34 odst. 2 GDPR.
[111] Ust. čl. 33 odst. 3 GDPR.

svou činností pomoci správcům a zpracovatelům při zpracování dosáhnout náležité ochrany osobních údajů. Jsou povinni poskytovat odbornou podporu a pomoc svým zaměstnavatelům nebo klientům tak, aby při své činnosti řádně splnili všechny povinnosti, které jim stanovuje zároveň GDPR i vnitrostátní předpisy. Za poskytnutí své odborné činnosti sice nesou odpovědnost, avšak dojde-li k porušení předpisů na ochranu osobních údajů, jehož důsledkem vznikne újma fyzické nebo právnické osobě, odpovídá za odčinění takovéto újmy zaměstnavatel či klient pověřence. Teprve ten může prostřednictvím regresního nároku požadovat náhradu své škody po pověřenci, prokáže-li pověřencovu vinu na vzniku škody.

Podle čl. 37 GDPR musí pověřence jmenovat všechny orgány veřejné moci a veřejné subjekty, s výjimkou soudů jednajících v rámci svých soudních pravomocí. Dále musí pověřence jmenovat osoby, jejichž hlavní činností jako správce nebo zpracovatele je zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů. Nakonec pak osoby, jejichž hlavní činnost spočívá v rozsáhlém zpracování zvláštních kategorií údajů podle čl. 9 nebo osobních údajů týkajících se rozsudků v trestních věcech podle čl. 10 GDPR, a dále subjekty, které v rámci své hlavní činnosti systematicky a rozsáhle monitorují jednotlivce.

Zde vzniká problém vymezení termínů orgán veřejné moci a veřejný subjekt. Podle zákona o základních registrech by se dal za orgán veřejné moci považovat státní orgán, územní samosprávný celek a fyzická nebo právnická osoba, byla-li ji svěřena působnost ve veřejné správě. Logicky je tedy možno za orgán veřejné moci považovat Policii ČR[112], odborovou organizace[113] a snad i osobu finančního arbitra[114]. Za veřejný subjekt je považován orgán zřízený zákonem nebo na základě zákona v oblasti práva veřejného, který plní zákonem stanovené úkoly ve veřejném zájmu. Lze tedy dovodit, že význam pojmů veřejný subjekt a orgán veřejné moci se mají blížit.

GDPR nedefinuje, kdy se o rozsáhlé zpracování osobních údajů jedná a kdy nikoli. Nicméně to ani definovat nelze a je nutné tento pojem aplikovat na každý případ samostatně. Vodítkem může být doporučení pracovní skupiny WP29, které bere při určení rozsahu v úvahu následující faktory – počet

[112] Rozhodnutí Nejvyššího osudu ČR sp. zn. 15 Tdo 574/06 ze dne 28. června 2006.
[113] Nález ÚS publikován pod č. 116/2008 Sb., nález Ústavního soudu ze dne 12. března 2008 ve věci návrhu na zrušení některých ustanovení zákona č. 262/2006 Sb., zákoník práce.
[114] Rozhodnutí Nejvyššího soudu ČR sp. zn. 25 Cdo 4744/2010 ze dne 26. ledna 2012.

dotčených subjektů, objem nebo rozsah dat, trvání nebo stálost zpracování a územní rozsah zpracování. Za příklady rozsáhlého zpracování pak považuje např. zpracování osobních údajů pacientů nemocničním zařízením, zpracování zákaznických dat v rámci pojišťovny nebo banky, zpracování poskytovatelem internetových nebo telefonních služeb. Za rozsáhlé zpracování naopak nepovažuje zpracování údajů o pacientech jednotlivými lékaři a zpracování informací o klientech jedním advokátem.

Pravidelné a systematické monitorování taktéž není v GDPR upraveno. Skupina WP29 vykládá výraz „pravidelný" jako kombinaci více variant. Jeho význam tedy může být např. stále se opakující nebo opakovaný ve stanoveném čase, průběžný nebo v pravidelných intervalech a po určitou dobu se opakující aj. Výraz „systematický" pak může znamenat např. vyskytující se podle určitého systému, přednastavený, organizovaný nebo metodický apod.[115]

Smyslem čl. 37 GDPR je lépe chránit osobní údaje v případech, kdy je postavení mezi subjektem údajů a správcem značně nevyrovnané. Pověřenec musí být jmenován vždy, kdy je jeho jmenování povinné podle čl. 37 odst. 1 GDPR. Není-li zjevné, zda má být pověřenec jmenován, doporučuje WP29 provedení interní analýzy ochrany osobních údajů[116], s jejíž pomocí by měl být správce či zpracovatel schopen určit, zda je jmenování nutné či nikoli. O předložení analýzy může být správce nebo zpracovatel požádán Úřadem pro ochranu osobních údajů. Zároveň má povinnost tuto analýzu průběžně aktualizovat. Pověřenec samozřejmě může být jmenován i v případech, kdy to povinné není, v některých případech je totiž jeho přítomnost logická, přestože není vyžadována. I v případě jeho dobrovolného jmenování zůstávají pověřenci stejné úkoly i působnost podle čl. 37 až 39 GDPR. Pověřenec je správcem či zpracovatelem ustaven pro všechny jejich činnosti týkající se zpracování osobních údajů.

Určujícím kritériem pro povinnost jmenování pověřence je povaha hlavní činnosti správce či zpracovatele. Zpracování skutečně musí být hlavní činností a ne jen činností pomocnou. Za hlavní činnost jsou tedy považovány klíčové operace nezbytné k dosažení cílů správce nebo zpracovatele, pro které byl stanoven, nebo které jsou jeho podnikatelskou činností. Jako příklad zde uvádí WP29 nemocnici, jejíž hlavní činnost sice spočívá v poskytování zdravotnické

[115] Pokyny týkající se pověřenců pro ochranu osobních údajů. *Uoou.cz* [online]. 2016, s. 9–10 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880
[116] Tamtéž, s. 6.

péče pacientům, avšak ta nemůže být řádně poskytnuta bez zpracování jejich zdravotních dat.

Povinnost jmenovat pověřence je pro správce i zpracovatele stejná. Můžou zde nastat tři situace – povinnost jmenovat pověřence má jen správce a nikoli zpracovatel, povinnost jmenovat pověřence má zpracovatel a nikoli správce, nebo mají povinnost jmenovat pověřence oba. V případě povinnosti obou jmenovat pověřence, pak musí jednotliví pověřenci spolupracovat. Existuje také možnost jmenování společného pověřence pro skupinu podniků, a to podle článku 37 odst. 2 GDPR, avšak to je možné pouze v případě, že bude pověřenec snadno dosažitelný pro každý podnik. Dosažitelnost se vztahuje na jeho povinnost být kontaktním bodem pro subjekty údajů. Orgány dozoruje i pro organizaci samotnou. Aby mohl být pověřenec společný, musí být schopen zvládnout tuto agendu nejen z hlediska objemu přidělené práce, ale také z hlediska času a dostupnosti. Pro dosažitelnost je lepší, aby pověřenec sídlil v EU bez ohledu na to, zda v ní sídlí správce nebo zpracovatel. V rozporu s požadavkem dosažitelnosti by byla také jeho přílišná vzdálenost od lokálního ústředí podniku. Jeho dosažitelnost je důležitá zejména pro povinnost bezodkladné reakce v případě porušení zabezpečení osobních údajů. Tehdy má totiž správce pouhých 72 hodin na to, aby o tomto porušení informoval Úřad pro ochranu osobních údajů, přičemž překročit tuto lhůtu lze jen v ojedinělých případech. Pro řádný výkon jeho funkce však není nutné, aby byl neustále přítomen na místě, kde se osobní údaje nachází nebo zpracovávají. Postačí, bude-li rychle dosažitelný prostřednictvím telefonu nebo jiného elektronického spojení. Podmínkou výkonu funkce pověřence je i jeho jazyková vybavenost, tudíž schopnost komunikovat nejen s pracovníky správce či zpracovatele, ale také se subjekty údajů nebo s Úřadem pro ochranu osobních údajů. Znamená to také nutnost být schopen komunikovat ve více cizích jazycích, minimálně v jazyce většiny subjektů údajů, velmi užitečnou také může být i znalost anglického jazyka, případně dalších jazyků.

Problém nastává v okamžiku, kdy je nutné zvolit, zda pověřencem zvolit externistu nebo jej přijmout do pracovního poměru. Obě varianty skýtají řadu výhod i nevýhod. Zaměstnanecký poměr bude mít zajisté výhodu v případě každodenního styku pověřence se zaměstnavatelem a v jeho znalosti provozu a činnosti zaměstnavatele, nevýhodou pak bude např. čerpání dovolené a řešení jeho případné zastupitelnosti, protože pověřenec může být jen jeden, a také

v okamžiku jeho případné výpovědi. Na externí pracovníky naopak neplatí omezení zákoníku práce jako např. čerpání dovolené nebo délka pracovní doby, existuje také možnost ho prakticky kdykoli vyměnit atd. Nevýhodou pak může být jeho nedostatečná znalost činnosti klienta nebo nedostatečný kontakt s pracovníky, popř. jeho každodenní nepřítomnost na pracovišti aj.[117] Podle WP29 je možné najmout pověřence i na základě smlouvy o poskytování služeb, která by měla mít formu smlouvy příkazní[118] nebo smlouvy inominátní[119].

Výhodou takovéto smlouvy může být zejména odborné a personální zázemí nasmlouvané společnosti, kdy zastupitelnost jednotlivých pověřenců zde nebude problémem. Důležité by pak bylo především definování náležitostí smlouvy, zejména pak možnost zastoupení pověřence, předmět smlouvy, cena popř. způsob jejího určení, odpovědnost za škodu, pojištění pověřence, otázky případného konfliktu zájmů apod.[120]

Článek 37 odst. 5 GDPR stanoví, že: „*pověřenec musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany osobních údajů a své schopnosti plnit úkoly stanovené v článku 39.*“

Prvním požadavkem je samozřejmě znalost práva, přičemž pověřenec by skutečně měl být odborníkem, a to především v otázkách práva na ochranu osobních údajů nejen na vnitrostátní, ale i evropské úrovni. Zároveň by měl být schopen rozlišit, zda se jedná o ochranu osobních údajů nebo o ochranu osobnostních práv v rámci soukromého práva. Druhým požadavkem je předpoklad odborné praxe v oblasti ochrany osobních údajů, poněvadž je nutné znát tuto problematiku nejen z teoretického hlediska, ale je potřeba mít dostatečné praktické zkušenosti. Samotná úroveň znalostí není v GDPR přesně stanovena, avšak měla by odpovídat tomu, v jaké oblasti bude pověřenec působit, popř. jak zásadní a komplikované situace bude řešit.

Článek 37 odst. 7 GDPR dále dává správci či zpracovateli povinnost zveřejnit kontaktní údaje jejich pověřence, a to především proto, aby mohly nejen subjekty údajů, ale také Úřad pro ochranu osobních údajů pověřence přímo kontaktovat. Pověřenec v rámci výkonu své činnosti podléhá ustanovením

[117] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 254–262.
[118] § 2430 a násl. zákona č. 89/2012 Sb., občanský zákoník.
[119] § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník.
[120] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 258–266.

týkajícím se povinnosti mlčenlivosti nebo dodržování služebního tajemství podle práva národního i práva EU. Článek 38 odst. 6 GDPR dává pověřencům možnost plnit i jiné úkoly a povinnosti než jen ty, zmíněné v čl. 39. Musí však být zajištěno, aby jejich plnění nevedlo ke střetu zájmů. Z toho vyplývá, že pověřenec nemůže zároveň zastávat pracovní místo, na kterém by stanovoval účel a prostředky zpracování osobních údajů.

Podle článku 38 GDPR musí „*správce a zpracovatel zajistit, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů*." V případě vypracování posouzení vlivu jsou správce a zpracovatel taktéž povinni vyžádat si k němu posudek pověřence. Pověřenec by měl být také zván schůze, kde bude docházet k rozhodnutím týkajícím se ochrany osobních údajů, správce a zpracovatel by měli dbát jeho připomínek a přiřknout jim dostatečnou závažnost. Také by s ním měl být bezodkladně konzultován jakýkoli případ porušení zabezpečení. V recitálu 97 GDPR se říká, že: „*pověřenci by měli být schopni, bez ohledu na to, zda se jedná o zaměstnance správce, plnit své povinnosti a úkoly nezávisle*." Při plnění svých úkolů podle článku 39 by tedy neměli pověřenci přijímat žádné pokyny, jak se mají s daným problémem vypořádat, např. jakého výsledku mají dosáhnout apod.

Podle znění článku 38 odst. 3 GDPR by neměli být pověřenci za plnění svých úkolů správcem nebo zpracovatelem sankcionováni nebo propuštěni. Toto ustanovení má posílit samostatnost a nezávislost pověřenců. Tresty podle GDPR však nelze pověřenci uložit jen v případech, kdy by k jejich uložení došlo následkem výkonu povinností pověřence. GDPR dále neupřesňuje, v jakých případech může být konkrétní pověřenec propuštěn nebo nahrazen jinou osobou. V případě nutnosti by tedy bylo nutné obrátit se na národní předpisy, zejména s ohledem na to, v jakém poměru by byl pověřenec ke správci či zpracovateli. Je však zjevné, že nahrazení externisty je rozhodně jednodušší než nahrazení pověřence ve stávajícím pracovním poměru. I to by však bylo možné v případě naplnění podmínek pro skončení pracovního poměru podle zákoníku práce.[121]

Jedním z úkolů pověřence je podle článku 39 odst. 1 písm. b) GDPR monitorování souladu se samotným GDPR. Pověřenec může v rámci svých povinností zejména shromažďovat informace za účelem zajištění

[121] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 267–277.

zpracovatelských činností, prověřovat a analyzovat právní soulad činností, informovat, radit a vydávat doporučení správci nebo zpracovateli.[122] Podle recitálu 97 GDPR by měl být pověřenec *„nápomocen správci nebo zpracovateli při monitorování toho, zda je zajištěn vnitřní soulad s tímto nařízením.“* Tato povinnost však nezakládá odpovědnost pověřence za případný nesoulad. Odpovědnost za nesoulad stále náleží správci, který je podle článku 24 odst. 1 GDPR povinen *„zavádět vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením.“*

V případě, že si správce při posuzování vlivu vyžádá od pověřence posudek, je povinen ho poskytnout. Tuto povinnost mu ukládá článek 39 odst. 1 písm. c) GDPR, který říká, že pověřenec je povinen *„poskytovat poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35.“* Pracovní skupina WP29 pak doporučuje správcům, aby vyžadovali posudek pověřence například v případech, kdy je to potřebné pro posouzení vlivu, není-li si správce jistý, zda posouzení vlivu vypracovat, zda bylo posouzení vlivu vypracováno správně nebo v případě, kdy je nutné uplatnit ochranná opatření pro zmírnění rizik aj.[123]

Pověřenec je taktéž povinen spolupracovat s Úřadem pro ochranu osobních údajů a působit jako jeho kontaktní prvek v záležitostech týkajících se zpracování a případné konzultace podle čl. 39 odst. 1 písm. d) a e) GDPR. Pověřenec jako kontaktní osoba usnadňuje Úřadu nejen přístup k dokumentům a informacím podle čl. 57, ale také výkon jeho vyšetřovacích, nápravných, povolovacích a poradních pravomocí podle čl. 58 GDPR. Pověřenec sice podléhá ustanovením o mlčenlivosti, tento fakt mu však nebrání v kontaktu Úřadu a požádání o jeho radu.

Podle čl. 30 odst. 1 a 2 GDPR je správce povinen „*vést záznamy o činnostech zpracování, za něž odpovídá*“ a zpracovatel povinen „*vést záznamy o všech kategoriích činností zpracování prováděných pro správce.*“ Pověřenec však často v rámci své činnosti registr operací zpracování vede, ten pak následně může správce či zpracovatel využít. Je však nutné si uvědomit, že pověřenec

[122] Pokyny týkající se pověřenců pro ochranu osobních údajů. *Uoou.cz* [online]. 2016, s. 20 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880
[123] Tamtéž, s 20.

za nedodržování GDPR nenese odpovědnost. Došlo-li by tedy v případě vedení záznamů k nesouladu, plně by za to odpovídal správce nebo zpracovatel.[124,125]

[124] Pokyny týkající se pověřenců pro ochranu osobních údajů. *Uoou.cz* [online]. 2016, s. 21–22 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31880

[125] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 277–282.

5. VNITROSTÁTNÍ PRÁVNÍ ÚPRAVA

Na našem území byla ochrana soukromí nejprve ustavena zákonem č. 87/1862 Sb. z.s., o ochraně svobody osobní a zákonem č. 88/1862 Sb. z.s., na ochranu svobody domovní. Po vzniku samostatného Československa byl přijat Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního.

Až v 90. letech 20. století u nás došlo k podrobnější kodifikaci osobních údajů. Nejprve tak učinil zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, a následně pak Listina základních práv a svobod (dále jen pod zkratkou „LZPS"), vyhlášená Usnesením předsednictva České národní rady č. 2/1993 Sb.

Teprve v roce 2000 byl přijat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který platí dodnes. Počátkem roku 2009 pak vstoupila v platnost Lisabonská smlouva, která novelizovala Smlouvu o Evropské unii.[126]

5.1 Právo na soukromí

Pojem ochrana osobních údajů přímo souvisí s právem na soukromí, které patří mezi základní lidská práva a je zaručeno nejen naším ústavním pořádkem, ale také mezinárodními předpisy. Součástí našeho ústavního pořádku je i LZPS, která v článku 7 odst. 1 zakotvuje nedotknutelnost osoby i jejího soukromí, přičemž výslovně stanoví, že toto právo může být omezeno jen na základě zákona.[127] Do práva na ochranu soukromí řadíme práva vymezená nejen v čl. 10, konkrétně právo na soukromí a rodinný život a právo na ochranu jména, příjmení, lidské důstojnosti, osobní cti a dobré pověsti, ale i právo na nedotknutelnost obydlí, tedy ochranu domovní svobody v čl. 12 a právo na ochranu listovního tajemství v čl. 13 a dále také práva obsažená v článcích 15 a 16.[128]

Právo na ochranu osobních údajů z práva na soukromí přímo vychází, proto je jeho vymezení a definice velmi důležitá. Tento pojem však překvapivě není v českém právu definován a jeho význam je tak často dovozován

[126] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 28.
[127] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 58.
[128] Listina základních práv a svobod.

z judikatury. Z rozhodnutí Městského soudu v Praze sp. zn. 7 Ca 204/2005 ze dne 28. února 2007 vyplývá, že: *„i prostory mimo obydlí se považují za soukromé“*, přičemž toto rozhodnutí dále odkazuje na judikaturu Evropského soudu pro lidská práva, která říká, že nelze limitovat soukromí pouze na vnitřní okruh, v němž jednotlivec může žít svůj soukromý život podle svých představ.[129] Popis tohoto pojmu můžeme nalézt také ve stanovisku č. 6/2009 Úřadu pro ochranu osobních údajů, kde bylo soukromí popsáno jako osobní, intimní sféra člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského stvoření. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce a součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.[130]

V případě ochrany osobních údajů dochází zpravidla ke střetu dvou hodnot. Na jedné straně stojí bezpečnost, ochrana majetku, života a zdraví, na straně druhé pak ochrana svobody, lidské důstojnosti a soukromí.[131] V takovém případě je nutno tato základní práva poměřit pomocí testu proporcionality, na jehož základě bychom měli dojít k závěru, které právo či svoboda má být zvýhodněno oproti druhému. Tento princip je založen na třístupňovém testu, který se používá při rozhodovací činnosti Evropského soudu pro lidská práva, Soudního dvora Evropské unie i Ústavního soudu, popř. Nejvyššího správního soudu, např. nález Ústavního soudu ČR sp. zn. Pl. ÚS 4/94 ze dne 12. října 1994 či novější nález sp. zn. Pl. ÚS 40/08 ze dne 26. května 2009. Omezit základní práva a svobody lze pouze na základě testu proporcionality a to jedině tehdy, jde-li o zásah, který je pro dosažení sledovaného cíle vhodný, nutný a přiměřený. Kritériem pro nutný zásah je skutečnost, že subjekt nemůže pro dosažení svého cíle použít jiný, objektivně srovnatelný prostředek, jímž by došlo k menšímu zásahu do chráněných zájmů na straně dotčeného subjektu údajů. Za přiměřený je považován takový zásah, kdy lze očekávat, že prospěch vzniklý z realizace dané činnosti bude větší než nepříznivý následek jí způsobený, spočívající zejména v zásahu do osobnosti dotčených subjektů údajů.

---

[129] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích.* Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 59.

[130] Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009. Ochrana soukromí při zpracování osobních údajů. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/stanovisko-c-6-2009-ochrana-soukromi-pri-zpracovani-osobnich-udaju/d-1519

[131] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 65.

S ochranou osobních údajů je pak nejblíže spjat obsah čl. 10 odst. 3 LZPS, který říká, že: *„každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“* Z tohoto sdělení nám tedy vyplývá právo osoby utajovat informace vztahující se k jeho osobě a současně i možnost obrany proti zásahům do tohoto práva, nedal-li dotyčný k manipulaci s tímto právem předchozí souhlas, nebo jestliže sám informaci nezveřejnil.

5.1.1 Soukromí zaměstnance na pracovišti

Zaměstnanci mají legitimní a ústavně zakotvený nárok na příznivé pracovní prostředí a podmínky, to je zakotveno nejen ve vnitrostátní úpravě v čl. 28 LZPS, který říká, že: *„zaměstnanci mají právo na spravedlivou odměnu za práci a na uspokojivé pracovní podmínky, přičemž podrobnosti o nich stanoví zákon.“* v souvislosti s čl. 31 LZPS: *„Každý má právo na ochranu zdraví. Občané mají na základě veřejného pojištění právo na bezplatnou zdravotní péči a na zdravotní pomůcky za podmínek, které stanoví zákon.“*, ale také v mezích mezinárodního práva v čl. 7 Mezinárodního paktu o hospodářských, sociálních a kulturních právech a v čl. 28 Všeobecné deklarace lidských práv. Na zákonné úrovni je pak právo na uspokojivé pracovní podmínky ukotveno v zákoníku práce například v ustanovení § 224 týkajícího se povinnosti zaměstnavatele vytvářet pro zaměstnance pracovní podmínky, které mu umožní bezpečný výkon práce nebo v § 227 až § 235, které upravují odborný rozvoj zaměstnanců aj. Další pravidla týkající se pracovního prostředí můžou být sjednána v interním předpise, v kolektivní smlouvě nebo ve smlouvě pracovní.

Vzhledem ke stále narůstající životní úrovni se dnes do pojmu příznivé pracovní podmínky neřadí pouze podoba pracovního prostředí, jako je kupříkladu hladina hluk a dostatečné osvětlení na pracovišti, ale také ochrana soukromí a rozvoj zaměstnance. Podle názoru ESLP není dost dobře možné přesně oddělit soukromý a profesní život, neboť hranice mezi nimi je velmi tenká především proto, že právě v rámci zaměstnání a pracovních aktivit má většina lidí největší možnost navazovat a dále rozvíjet kontakty a vztahy s jinými lidmi. Není tedy

snadné rozlišit, jestli dané činnosti nebo vztahy spadají ještě do sféry profesní či nikoli.[132]

Zaměstnanec má tedy právo na ochranu soukromí i přímo na pracovišti, je totiž potřeba chránit jeho důstojnost. Zaměstnanec má však primárně povinnost trávit svou pracovní dobu výkonem práce a soukromými aktivitami se může zaobírat jen v případě, je-li to nezbytně nutné, nebo jestliže mu to zaměstnavatel výslovně povolil. Zaměstnavatel je, podle § 316 odst. 1 zákoníku práce, který říká, že: *„zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení.“* oprávněn přiměřeným způsobem kontrolovat výkon práce, která byla zaměstnanci přidělena, i způsob nakládání se svěřeným majetkem zaměstnavatele. Avšak podle odst. 2 *„nesmí zaměstnavatel bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.“*[133]

5.2 Občanský zákoník

Již z úvodních ustanovení zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, lze vyvodit fakt, že celé soukromé právo spočívá na základech ochrany soukromí člověka. Ochranu před jednorázovými zásahy do soukromí jednotlivce upravuje především § 81 a násl. NOZ v rámci institutu ochrany osobnosti člověka.[134] Rovněž je zde obecně upraveno právo dotčené fyzické osoby domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn následek, který tímto zásahem do soukromí dotčené osoby vznikl.[135] Lze se také prostřednictvím tzv. satisfakční žaloby domáhat náhrady škody nebo nemajetkové újmy, která byla způsobena v rámci nevhodného způsobu zpracování osobních údajů.

[132] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 66–69.
[133] KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013. ISBN 978-80-7273-173-2, s. 140–149.
[134] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7, s. 283–284.
[135] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

5.3 Zákon o ochraně osobních údajů

Tento zákon byl přijat v souvislosti se vstupem ČR do EU, přičemž měl reflektovat evropskou úpravu ochrany osobních údajů, skládající se především z Úmluvy č. 108 a směrnice 95/46/ES. Smyslem tohoto zákona je ochrana základního lidského práva vyplývajícího z čl. 10 odst. 3 LZPS, neboli práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě, které je nedílnou součástí práva na ochranu soukromí.

Z hlediska pozitivního vymezení osobní a věcné působnosti se zákon o ochraně osobních údajů vztahuje na veškeré zpracování osobních údajů, bez ohledu na jeho prostředky a bez ohledu na to, zda je prováděno státními orgány, orgány územní samosprávy, jinými orgány veřejné moci, či fyzickými anebo právnickými osobami. V pracovněprávním vztahu má stát postavení právnické osoby. Zmíněný zákon se použije v případě, dochází-li k systematické manipulaci s prvky osobní povahy či jinými informacemi týkajícími se konkrétní fyzické osoby, přičemž tento proces by se dal nazvat zpracováním osobních údajů. Vztahuje se na automatizované i manuální zpracování údajů. Najdeme zde i vymezení negativní, které stanovuje, na které zpracování se tento zákon nevztahuje.[136] Vedle působnosti věcné a personální je v § 3 taktéž vymezena působnost místní, kdy se zákon o ochraně osobních údajů může použít na základě mezinárodní smlouvy i na správce, který nesídlí v České republice.

Jednotlivým ustanovením tohoto zákona se věnuji v průběhu celé své práce, zejména v předcházejících kapitolách, proto je zde nebudu znovu rozebírat.

5.4 Zákoník práce

Současná úprava zákoníku práce ve vztahu k občanskému zákoníku stojí na principu subsidiarity. Subsidiarita je založena na právním principu „*lex specialis derogat legi generali*“. Existuje-li tedy úprava dané problematiky ve speciálním předpise, použije se ten namísto úpravy obecné.

Zaměstnavatel má v zákoníku práce stanoveny některé povinnosti týkající se osobních údajů. Vzhledem k tomu, že mu tyto povinnosti vyplývají přímo ze zákona, není povinen jejich zpracování oznamovat Úřadu pro ochranu osobních údajů v rámci své oznamovací povinnosti. Jedná se zejména o zpracování osobních údajů prostřednictvím vedení evidence pracovní doby

[136] Ust. § 1 až § 3 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

podle § 96 zákoníku práce nebo vedením knihy úrazů a evidence nemocí z povolání podle § 105 odst. 2 a 6 zákoníku práce. Můžeme zde také nalézt ustanovení, které zaměstnavatele zpracovávat osobní údaje zaměstnanců opravňuje, avšak neukládá mu to jako povinnost, jedná se například o vedení osobního spisu zaměstnance podle § 312 zákoníku práce aj.

Speciální úpravu týkající se osobních údajů v pracovněprávních vztazích nalezneme především v § 316, který tvoří celou Hlavu VIII. zákoníku práce. Zákoník práce upravuje také některá další práva zaměstnanců jakožto subjektů údajů a povinnosti a oprávnění zaměstnavatele. Další ustanovení dotýkající se ochrany soukromí a osobních údajů nalezneme například v zákoně o zaměstnanosti, v zákoně č. 155/1995 Sb., o důchodovém pojištění, zákoně č. 187/2006 Sb., o nemocenském pojištění, a v dalších právních předpisech.[137]

[137] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 171–174.

6. SOUČASNÁ ÚPRAVA OCHRANY OSOBNÍCH ÚDAJŮ V PRACOVNĚPRÁVNÍCH VZTAZÍCH

Účelem ochrany osobních údajů v pracovněprávních vztazích by mělo být zajištění toho, aby měl zaměstnavatel právo shromažďovat a dále zpracovávat osobní údaje zaměstnance v rozsahu nezbytném pro realizaci svých práv a plnění svých povinností, které mu vyplývají ze zvláštních právních předpisů. Na základě získaných osobních údajů nesmí nikdy dojít k diskriminaci zaměstnance ze strany zaměstnavatele. Pracovněprávní vztahy jsou tedy upraveny několika oblastmi zákonů. Zákonem o ochraně osobních údajů, jenž zastává pozici generálního právního přepisu, zákoníku práce jako právního předpisu speciálního, občanského zákoníku, který zakotvuje především problematiku ochrany osobnosti a dalšími speciálními právními předpisy, jako například zákon o důchodovém pojištění, zákon o zaměstnanosti, zákon o nemocenském pojištění atd.[138]

Zpracování osobních údajů zaměstnance zaměstnavatelem lze rozdělit do fází zpracování z hlediska trvání pracovního poměru na zpracování před jeho vznikem, při vzniku a za trvání pracovního poměru a po jeho skončení. Nejobsáhlejší je pak kategorie druhé fáze, ve které dochází například ke zpracování osobních údajů pro účely mzdové a personální agendy, k vedení evidence dovolené a knihy úrazů nebo k evidenci pracovní doby.

Zpracování osobních údajů v pracovněprávních vztazích může být obligatorní nebo fakultativní. Obligatorně stanovuje zaměstnavateli povinnost zpracování zákon, fakultativně rozhoduje zaměstnavatel o zpracování osobních údajů sám, přičemž účel zpracování vyplývá z příslušného právního předpisu, nebo si ho zaměstnavatel sám určí. Nejčastějším případem fakultativního zpracování je provozování kamerového systému se záznamem v rámci provozovny zaměstnavatele. V případě fakultativního zpracování zde existuje povinnost zaměstnavatele každé takovéto zpracování ohlásit Úřadu pro ochranu osobních údajů. Obligatorní zpracování oznamovací povinnosti nepodléhá.[139]

[138] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 50–57.
[139] Tamtéž, s. 174–175.

6.1 Změny související s přijetím GDPR

Přestože přijetí GDPR bylo ze strany médií značně zveličováno, je nutné podotknout, že se toto obecné nařízení od směrnice 95/46/ES příliš neodlišuje. Samo nařízení stanovuje, že cíle a zásady směrnice platí i nadále. Řada základních pojmů je v GDPR i ve směrnici upravena obdobně, někdy dokonce shodně. Přestože GDPR mělo úpravu osobních údajů na poli EU sjednotit, dává v mnoha svých ustanoveních povinnost nebo alespoň možnost členským státům upravit vymezenou problematiku ve vnitrostátním právu samostatně, avšak v mezích GDPR.

Pro pracovněprávní vztahy je zde důležitá možnost členských států zavést konkrétnější podmínky zpracování osobních údajů v případech, kdy je právním titulem pro zpracování osobních údajů plnění právních povinností správce.[140] Článek 88 odst. 1 GDPR pak umožňuje členským státům prostřednictvím právního předpisu anebo kolektivní smlouvy *„stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, 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 individuál-ního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.“*

Pravidla přijatá na základě tohoto ustanovení však musí také obsahovat vhodná opatření, jež by sloužila k ochraně lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, zejména v případech transparentnosti zpracování, předávání údajů v rámci podniku a monitorovacích systémů na pracovišti.[141] Na základě výše uvedeného lze tedy říci, že GDPR se bude vztahovat i na pracovněprávní vztahy, avšak bude-li přijata speciální právní úprava jednotlivých ustanovení, bude mezi GDPR a speciálním předpisem uplatňována zásada lex specialis derogat legi generali.[142] Tato zásada se využije například u čl. 15 GDPR, který zakotvuje právo subjektu údajů *„požadovat*

[140] Ust. čl. 6 odst. 2 GDPR.
[141] Ust. čl. 88 odst. 2 GDPR.
[142] Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů. *Bulletin-advokacie.cz* [online]. 2017 [cit. 2019-03-18]. Dostupné z: http://www.bulletin-advokacie.cz/reforma-ochrany-osobnich-udaju-v-eu-z-pohledu-pracovnepravnich-vztahu

po správci jednak potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud ano, pak má právo na přístup k osobním údajům a k informacím vyjmenovaným v čl. 15 odst. 1 GDPR" a ustanovení § 312 zákoníku práce, které upravuje vedení osobního spisu zaměstnance, jeho odst. 3 pak stanovuje právo zaměstnance do osobního spisu nahlížet, pořizovat si z něho opisy dokladů v něm obsažených, a to všechno na náklady zaměstnavatele. Vzhledem k tomu, že zákoník práce je tedy vůči GDPR v postavení lex specialis, použije se § 312 zákoníku práce namísto čl. 15 GDPR.

Zpracování osobních údajů nad rámec stanovený zákonem je podmíněno souhlasem zaměstnance již nyní. Úpravou problematiky souhlasu jsem se zabývala v kapitole 3.3 a změnám v něm v kapitole 5.6. Podle GDPR však tento souhlas již v zásadě nebude možné udělit a zaměstnavatel tak bude moci osobní údaje zpracovávat jedině na základě zákonných důvodů. Zákoník práce je přitom v této oblasti dosti štědrý a stanovuje zaměstnanci i zaměstnavateli celou řadu povinností, které se nedají bez zpracování osobních údajů splnit. Nově se v GDPR upravuje možnost zaměstnance podat námitku, při jejímž uplatnění by zaměstnavatel musel zpracování údajů okamžitě přerušit nebo ukončit. To může zaměstnavatelům způsobit velké problémy například při předávání osobních údajů v rámci firemních poboček či napříč celou firemní hierarchií.

Zpracování zvláštních kategorií osobních údajů, tedy kategorie známé v české úpravě pod pojmem citlivé údaje, je podmíněno výslovným souhlasem subjektu údajů. Pro pracovněprávní vztahy však bude toto zpracování spíše výjimečné, poněvadž souhlasu se zpracováním osobních údajů musí být využíváno střídmě. Článek 9 odst. 2 písm. a) GDPR pak výslovně dává členskému státu možnost vyloučit ze zpracování určité zvláštní kategorie osobních údajů na základě souhlasu jejich subjektu, byť výslovně projeveného. I nadále tak bude možné použít ustanovení §316 odst. 4 zákoníku práce, které vyjmenovává informace, jejichž sdělení nemůže zaměstnavatel po zaměstnanci v žádné situaci požadovat.

Další problém může vzniknout při řešení problematiky uchovávání životopisů uchazečů o zaměstnání, na kterou existují dva pohledy. První výklad předpokládá, že se na uchazeče o zaměstnání GDPR vztahovat bude, potom by bylo se souhlasem možné uchovat životopisy pouze těch uchazečů, kteří by na poli dané společnosti našli pracovní uplatnění, ostatní životopisy by musely být smazány. Naopak v případě, že by se na uchazeče a jeho životopis

nevztahovala úprava GDPR, pak by bylo stále možné souhlas s uchováním libovolného životopisu poskytnout.

Podle GDPR se tedy budou moci zaměstnavatelé na souhlas zaměstnance spolehnout jen zřídkakdy. Bude to možné jen v případě, kdy by konkrétní oprávněný zájem zaměstnavatele na zpracování osobních údajů výrazně převažoval nad povinností zachování soukromí zaměstnance. Bude tedy nutné provádět test proporcionality, a to mnohem intenzivněji a častěji, než je tomu nyní. Zaměstnavatel bude také povinen zpracovávat osobní údaje transparentně a o rozsahu zpracování zaměstnance podrobně informovat.

Zaměstnavatel nebude dále moci používat informace o zaměstnancích, které získal na sociálních sítích. Nelze totiž předpokládat, že ačkoli zaměstnanec informace sám o osobě dobrovolně zveřejnil, udělal to pro účely jejich využití současnými nebo budoucími zaměstnavateli. Aby užití těchto informací bylo legální, musel by o úmyslu zaměstnavatele projít jeho sociální média předem vědět, např. formou inzerátu. Odpověděl-li by na daný inzerát, toto by bylo možno považovat za udělení souhlasu s tzv. screeningem, avšak získané údaje by měly být ihned po vyřazení potencionálního uchazeče smazány. Nakonec však bude záležet na povaze dané sociální sítě.

Sledování zaměstnanců mimo pracoviště je vyloučeno úplně, např. skenování mobilního telefonu včetně soukromých souborů, a to i v případě, kdy se jedná o zařízení zaměstnavatele, které je využíváno v rozporu s jeho účelem. Skenování by bylo možné v případě, kdy by došlo k odlišení soukromých a služebních souborů. Rovněž by mělo být možné deaktivování sledování vozidla mimo pracovní hodiny nebo při jeho soukromém využívání. Zaměstnavatel by měl být schopen alespoň omezeného sledování vlastního majetku v případě, kdy by jeho využití pro soukromé účely zcela zakázal, případně mohlo-li by využitím daného zařízení dojít k ohrožení zabezpečení ochrany dat, např. pokud by zaměstnanec mohl zneužít dané zařízení k přístupu ke zpracovávaným citlivým údajům, za které nese zaměstnavatel odpovědnost. Za porušení bezpečnosti a pravidel zpracování osobních údajů zaměstnavateli nově hrozí velmi vysoké sankce.[143]

[143] GDPR zasáhne i do zákoníku práce. Na co se musí firmy připravit? *BusinessInfo.cz* [online]. 2018 [cit. 2019-03-17]. Dostupné z: https://www.businessinfo.cz/cs/clanky/gdpr-zasahne-i-do-zakoniku-prace-na-co-se-musi-firmy-pripravit-102429.html

6.2 Zpracování před vznikem pracovního poměru

Zaměstnavatel je povinen zpracovávat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu. Je tedy nutné vymezit konkrétní údaje, které bude zapotřebí ke splnění vymezeného účelu zpracovávat. Cílem je dosažení situace, kdy bude možné dosáhnout stanoveného účelu s co možná nejmenším okruhem osobních údajů. Správce by měl být také schopen kdykoli si zpracování konkrétního osobního údaje obhájit. Shromážděné údaje, které nebudou dále zpracovávány, by měly být neprodleně zničeny. Zaměstnavatelé tyto požadavky často nerespektují a již ve fázi zájmu o pracovní místo dochází ke zpracování nadbytečných osobních údajů uchazečů. Nejčastěji dochází ke zpracování osobních údajů, které by vůbec zpracovávány být neměly, případně by k jejich zpracování mělo dojít až po uzavření pracovní smlouvy.

Základním předpisem upravujícím vztahy mezi fyzickou osobou a potenciálním zaměstnavatelem je zákon č. 435/2004 Sb., o zaměstnanosti, zákoník práce a do jisté míry i zákon č. 234/2014 Sb., o státní službě. Zákonem o zaměstnanosti je přímo stanoveno, které údaje není ve fázi výběru uchazečů povoleno zjišťovat. Podle ustanovení § 12 odst. 2 zákona o zaměstnanosti *„zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu se zvláštním právním předpisem 80), dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem. Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje. Hlediska pro výběr zaměstnanců musí zaručovat rovné příležitosti všem fyzickým osobám ucházejícím se o zaměstnání.“*

Zákonodárce tedy tímto ustanovením vyloučil získávání citlivých údajů s výjimkou údaje o odsouzení za trestný čin, jeho potřebnost však bude muset zaměstnavatel prokazovat a lze jej požadovat jen v případě nutnosti. Toto ustanovení, týkající se citlivých údajů, však může být v některých případech prolomeno, konkrétně v případě § 103 odst. 1 písm. a), § 105 a § 286 odst. 6 zákoníku práce, kdy je informace o citlivých údajích pro zaměstnavatele klíčová. Například tehdy, je-li zvláštním předpisem vyžadována bezúhonnost budoucího zaměstnance. Rozsah osobních údajů, které může zaměstnavatel po uchazeči

o zaměstnání bez prokázání potřebnosti požadovat, může být značně omezen, a to toliko na informace bezprostředně se týkající obsazovaného místa. Bude tedy moci shromáždit identifikační údaje, jako jsou jméno, příjmení a datum narození, přičemž je nutné se vyvarovat jakékoli známce diskriminace, dále pak informace o vzdělání a praxi, zvláštní předpoklady vyžadované podle zvláštního předpisu a běžné kontaktní údaje jako telefonní číslo nebo e-mailová adresa.[144]

Ustanovení § 30 zákoníku práce zároveň 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*.“ Tato definice je sice poněkud obecná, avšak v souvislosti s ostatními ustanoveními, zejména ustanovením §316 zákoníku práce, lze říci, že se jedná o veškeré údaje, které jsou nutné pro to, aby byla nabídka práce ze strany zaměstnavatele právním jednáním se všemi jeho obligatorními náležitostmi. Prvotním účelem shromáždění těchto dat je tedy nalezení vhodného kandidáta pro nabízenou pozici.

6.3 Zpracování po dobu trvání pracovního poměru

Osobní údaje zaměstnance může zaměstnavatel v této fázi pracovního poměru zpracovávat buďto na základě zákonné povinnosti, zákonného povolení nebo na základě vlastního uvážení bez zákonné opory. Zákon o ochraně osobních údajů se v prvních dvou případech zpracování použije subsidiárně, v případech, kdy není některá povinnost speciálně upravena. Pro třetí skupinu, tedy pro zpracování osobních údajů bez zákonné opory, je zákon o ochraně osobních údajů právním předpisem primárním. Podstatné bude tedy to, že osobní údaje musí být vždy zpracovávané za účelem naplnění příslušného pracovního poměru nebo k realizaci práv subjektů, které s pracovním poměrem nějak souvisí nebo jsou od něho odvozené.[145]

Pokud bude zaměstnavatel zpracovávat osobní údaje zaměstnanců pouze za účelem vedení personální a mzdové agendy, přičemž mu je tato povinnost dána zvláštní zákonnou úpravou, pak oznamovací povinnosti podle § 16 zákona

[144] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 51–61.
[145] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 386–387.

o ochraně osobních údajů nepodléhá.[146] Vztahovala by se na něj pouze v případě, kdy by zaměstnavatel zpracovával osobní údaje svých zaměstnanců i za jinými účely, než těmi, které jsou mu přiřčeny zvláštními zákony, příp. pokud by zpracovával osobní údaje, jejichž zpracování podléhá obdržení souhlasu příslušného zaměstnance.[147] Souhlas zaměstnance však není třeba např. v případě poskytování osobních údajů o zaměstnanci Policii ČR.

Jak už bylo řečeno dříve, zákoník práce ve svém § 316 stanovuje zaměstnavateli dva zákazy, konkrétně zákaz narušování soukromí zaměstnance a zákaz vyžadování údajů, které nesouvisejí s výkonem práce. Zaměstnavatel tedy nesmí bez závažného důvodu narušovat soukromí zaměstnance tím, že by zaměstnance sledoval, odposlouchával a kontroloval. Právo zaměstnavatele na určitou kontrolu vyplývá z § 316 odst. 3 zákoníku práce, který říká že: *„jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění“*, není však dáno vždy, ale pouze v závislosti na povaze jeho činnosti. Majetkové zájmy zaměstnavatele jsou pak chráněny § 316 odst. 1, podle něhož nesmí zaměstnanci bez souhlasu zaměstnavatele používat pro osobní potřebu majetek zaměstnavatele jim svěřený, např. telekomunikační zařízení, služební automobil atd. Dodržování tohoto zákazu je oprávněn zaměstnavatel přiměřeně kontrolovat.[148]

Příkladem, kdy je zaměstnavatel povinen zpracovávat citlivé údaje zaměstnance je např. vedení evidence pracovních úrazů a nemocí z povolání. Vzhledem k tomu že tato povinnost je dána zákonem, nepotřebuje zaměstnavatel k opatření údajů o zdravotním stavu zaměstnance jeho výslovný souhlas. Osobní údaje zaměstnance, které zaměstnavatel shromáždil, jsou zpravidla po celou dobu trvání pracovního poměru obsaženy v tzv. osobní složce zaměstnance. Zákoník práce pak výslovně stanovuje, že její součástí mohou být jen ty dokumenty,

[146] Stanovisko Úřadu pro ochranu osobních údajů č. 6/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[147] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 62–67.
[148] Ochrana osobních údajů, služební zákon a sociální souvislosti zaměstnávání cizinců. Sborník příspěvků z mezinárodní vědecké konference. *Brno: Masarykova univerzita, 2018*. ISBN 978-80-210-8930-3, s. 82–87. Dostupné také z: https://www.law.muni.cz/sborniky/pracpravo2017/files/PracovniPravo2017.pdf

které jsou nezbytné pro výkon práce, jedná se např. o životopis, pracovní posudek, mzdový výměr apod.

6.3.1 Monitoring zaměstnanců

Pro monitoring zaměstnanců existují velmi přísná pravidla. Obecně platí, že k němu na pracovišti může dojít jen v případě, kdy to přímo ukládá právní předpis, nebo existuje-li pro to legitimní důvod spočívající zejména v ochraně majetku zaměstnavatele, zajištění bezpečnosti na pracovišti aj. Důležitá je zejména přiměřenost monitoringu, přičemž sledován může být jen cíl, za kterým bylo monitorování zřízeno. Dochází-li k monitorování pracoviště, musí o tom být zaměstnanci patřičně poučeni. Musí být taktéž seznámeni s rozsahem i účelem zpracování jejich osobních údajů takovým způsobem pořízených. V případě použití kamerového systému na pracovišti je pak zásadní, zda se jedná o kamerové zařízení se záznamem nebo bez záznamu. S provozem kamerového systému však musí být zaměstnanci seznámeni vždy. V případě provozu kamerového systému se záznamem platí nutnost jeho provoz předem ohlásit Úřadu pro ochranu osobních údajů, protože s využitím záznamů jím pořízených je možná následná identifikace jednotlivých osob.

Také v případě GPS ve služebních vozech musí být splněna legitimita jejího použití. GPS patří mezi oblíbené prostředky zaměstnavatelů, jak sledovat zaměstnance při výkonu jejich práce a při služebních cestách. Tak jako v předchozím případě však může být GPS použita jen v případě, pokud její využití sleduje zvláštní zájem zaměstnavatele, je-li její použití přiměřené a byl-li na její využití zaměstnanec upozorněn. V případě, že tedy byl konkrétnímu zaměstnanci svěřen do užívání služební vůz, přičemž jeho využívání bylo omezeno jen k výkonu stanoveného druhu práce, může toto užívání zaměstnavatel kontrolovat využitím GPS. Pokud by však zaměstnanci bylo dovoleno využívat služební vůz i k soukromým účelům, bylo by značně nepřiměřené sledování GPS využívat i mimo pracovní dobu zaměstnance, mohlo by tím totiž dojít k zásahu do soukromí zaměstnance, ke kterému by zaměstnavatel neměl legitimní důvod.

V případě sledování e-mailů je nutné rozlišit, zda se jedná o e-mailovou adresu soukromou, či nikoli. Obecně platí, že je-li e-mail zřízen na freemailovém serveru[149] nebo skládá-li se ze jména a příjmení zaměstnance,[150] jedná se o e-mail

[149] Např. seznam.cz, gmail.com apod.
[150] Např. jan.novak@seznam.cz nebo jan.novak@zamestnavatel.cz.

soukromý a zaměstnavatel tedy nemá oprávnění do něj nahlížet. Otevřít e-mail, který by se např. dle předmětu a odesílatele zdál pracovní, by mohl zaměstnavatel například v případě dlouhodobé nemoci zaměstnance nebo jeho nepřítomnosti z důvodu čerpání dovolené, a pouze tehdy, kdy by mu jeho nevyřízení mohlo způsobit škodu. E-maily s tzv. úřední elektronickou adresou[151] spadají do zvláštního režimu a zaměstnavatel je proto oprávněn do nich nahlížet bez omezení. Nejsou totiž považovány za soukromé nikdy, a to ani v případě, že jejich správa spadá výlučně do rukou jednoho zaměstnance.[152]

Velmi častým případem, kdy zaměstnavatelé mají potřebu kontrolovat zaměstnance, je také využití internetu v pracovní době, nejčastěji prostřednictvím svěřeného notebooku nebo počítače. Zaměstnanci si často neuvědomují, že využití věcí jim svěřených zaměstnavatelem pro osobní potřeby je bez souhlasu zaměstnavatele zakázáno, a tak svěřené věci využívají v pracovní době k vyřizování soukromých věcí, popř. k prohlížení internetových stránek aj. Užíval-li by však zaměstnanec svěřené věci pro osobní potřebu bez výslovného souhlasu zaměstnavatele, jednalo by se o porušení pracovních povinností, které by mohlo vést až k výpovědi z pracovního poměru. Přestože zaměstnavatel musí zaměstnance o možnosti sledování informovat a může tuto kontrolu realizovat jen přiměřeně a v odůvodněných případech, je nutno si uvědomit, že omezit využití internetu pro soukromé účely lze i jinak, např. prostřednictvím technického omezení přístupu na určité stránky, jako jsou sociální sítě, hry atd.[153] I zde je však nutné zvážit, zda by aplikace takovýchto opatření nekladla nepřiměřeně velké nároky na zaměstnavatele, spočívající zejména ve výši nákladů na provedení tohoto opatření.

Je také nutno říci, že není-li dán legitimní důvod pro sledování zaměstnance podle § 316 zákoníku práce, pak sledování provést nelze, a to ani v případě, že by k němu zaměstnanec svolil, ustanovení § 316 odst. 2 zákoníku práce je totiž ustanovením kogentním a nelze se tedy od něj odchýlit. Zaměstnanec se zároveň nemůže platně vzdát svých práv se závazkem do budoucna. Z výše uvedeného tedy vyplývá, že neoprávněný zásah do soukromí

[151] Např. office@domena.cz.
[152] Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: Dostupné z: https://www.uoou.cz/stanovisko-c-2-2009-ochrana-soukromi-zamestnancu-se-zvlastnim-zretelem-k-monitoringu-pracoviste/d-1511
[153] JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3, s. 85–96.

zaměstnance, nemůže být v žádném případě důvodem pro ukončení pracovního poměru ze strany zaměstnavatele.[154]

6.4 Osobní údaje zaměstnance po ukončení pracovního poměru

Možnost zaměstnavatele zpracovávat osobní údaj zaměstnance ani po skončení pracovního poměru ex lege v plném rozsahu nezaniká. I zde může být povinnost zpracování určitých osobních údajů dána zvláštním předpisem. Informace, které je zaměstnavatel povinen evidovat jsou stanoveny § 150 zákoníku práce, jedná se o jméno, popřípadě jména a příjmení, adresu, jde-li o fyzickou osobu, název a sídlo, jde-li o právnickou osobu, a dokumenty týkající se prováděných srážek ze mzdy, a to po shodnou dobu jako ostatní údaje a doklady týkající se mzdy či platu. Příkladem může být například povinnost zaměstnavatele vydat zaměstnanci po skončení pracovního poměru pracovní posudek podle § 314 a násl. zákoníku práce nebo povinnost vydat zaměstnanci zápočtový list podle § 313 zákoníku práce, přičemž k tomu, aby zaměstnavatel mohl své povinnosti dostát, potřebuje k jejich vypracování příslušná data.

Pro stanovení délky doby zpracování je i zde rozhodný jeho účel. Dále je pak ve vlastním zájmu zaměstnavatele určité informace archivovat proto, aby mohl prokázat řádné plnění svých povinností v oblasti daňové a sociálního zabezpečení. Má také právo uchovávat určité údaje proto, aby byl schopen se bránit v případném soudním sporu o neplatnost ukončení pracovního poměru nebo proti obvinění z diskriminačního jednání. Doba uchování těchto dat je dána během objektivních lhůt promlčecích a prekluzivních, není-li právním předpisem stanovena doba jiná.[155]

[154] Rozsudek Evropského soudu pro lidská práva ve věci 61496/08 - Bărbulescu proti Rumunsku ze dne 12. 1. 2016 a 5. 9. 2017.
[155] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1, s. 387–388.

ZÁVĚR

Cílem mé diplomové práce bylo přiblížení problematiky ochrany osobních údajů i právně nevzdělanému člověku. V intencích zákona o ochraně osobních údajů jsem vymezila rozdíly mezi osobním a citlivým údajem, kategorie citlivých údajů a jejich zpracování. Dále pak subjekty, které se na zpracování osobních údajů podílejí, definovala jsem pro tuto oblast stěžejní pojmy, jako je subjekt údajů, správce a zpracovatel a vysvětlila rozdíly mezi nimi. Popsala jsem jejich práva a povinnosti, která jsou jim zákonem o ochraně osobních údajů svěřena. V případě Úřadu pro ochranu osobních údajů jsem se zaměřila na jeho působnost a pravomoci a na jeho roli hlavního „dozorčího orgánu", již mu přiřklo GDPR.

Přestože zůstávají základní zásady zpracování osobních údajů až na malé odlišnosti vesměs stejné, přineslo s sebou GDPR také řadu změn a novot. Ohlašovací povinnost zpracovatele se změnila v povinnost konzultace s Úřadem pro ochranu osobních údajů, která má proces zpracování především urychlit a zajistit, aby v jeho průběhu nedošlo k nenadálým rizikovým událostem. V souvislosti s tím byla také zavedena nová povinnost vypracování posouzení vlivů zpracování na ochranu osobních údajů správcem, čímž by se mělo docílit eliminace většiny případných rizik. Nově je také správce povinen do 72 hodin nahlásit porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů.

Došlo však také k posílení některých práv subjektů údajů, zejména pak právní úprava souhlasu se zpracováním. Novým prvkem se stalo právo subjektu na výmaz, které je známo spíše pod spojením „právo být zapomenut", a právo subjektu podat námitku se zpracováním. Jejich případné uplatnění zpracovatelům zajisté přináší nejen noční můry, ale i značné náklady. Právo na námitku totiž, až na výjimečné situace, v podstatě znemožňuje správci pokračovat ve zpracování osobních údajů subjektu, který ji uplatnil. Právo na výmaz pak nutí správce, resp. zpracovatele k absolutní likvidaci osobních údajů subjektu, a to i těch, které předal jiným zpracovatelům.

Pro všechny je však zřejmě největší novem zavedení institutu pověřence pro ochranu osobních údajů, který má v rámci své činnosti kromě jiného dohlížet na zpracování údajů a jeho soulad s ustanoveními GDPR. Přestože se tento institut zdá být užitečným, podle mého názoru v tomto statutu existuje stále mnoho nezodpovězených otázek. Největším problémem se mně jeví nedostatečné určení požadavků na jeho vzdělání.

Nakonec bych ráda zmínila, že přestože GDPR zajisté reflektuje technologický pokrok, vzhledem k jeho poměrně krátké účinnosti nemohu s jistotou říci, jestli bude v konečném důsledku prospěšné či nikoli. Teprve čas a zodpovězení některých nejasností judikaturou ukáže jeho případné přínosy, a to i v rámci pracovněprávních vztahů. Domnívám se tedy, že se mi stanovený cíl s ohledem na možný rozsah mé práce podařilo naplnit.

RESUME

The protection of personal data is very current theme, particularly nowadays when technological progress is changing constantly. The aim of this thesis was to familiarize the reader with the issue of personal data protection and their processing in accordance with national and European law, mainly by using Act No. 101/2000 Coll., on Personal Data Protection and Regulation 2016/679, known as General Data Protection Regulation or shortly "GDPR". I also tried to apply the found knowledge about personal data to labor-law relations, mainly between employer and employee.

I tried to define the thin line that lies between personal and sensitive data and to show the difference between them. I also managed to define the difference between the individual entities involved in the processing of personal data, such as the data subject, the controller and the processor. Afterwards I focused on the new regulation known as GDPR and the changes that came with its efficiency.

The existing reporting duty has changed into the obligation to consult the Office for Personal Data Protection; there is also a new obligation to develop an assessment of an impact of personal data processing on their protection and an obligation to report a personal security breach to the Office for Personal Data Protection within 72 hours of its creation. Furthermore, even some rights of the data subjects were considerably strengthened, for example the consent to the processing of personal data was limited to exceptional situation. Other than that, the right to be forgotten and the subject´s right to object the processing of personal data, were also considered as novelties that came with GDPR.

However, the biggest novelty for everyone was probably the introduction of the Data Protection Officers, whose main activity should be to ensure the compliance between the data processing with GDPR provisions.

I think that even though accepting the GDPR was generally a good thing, its usability will be shown in the future. I also have to admit that its application on labor-law relations, shown to be quite a challenge for me so I mainly stayed in the known circuit of problems and tried to apply GDPR provisions adequately.

SEZNAM ZDROJŮ

Bibliografické zdroje

JANEČKOVÁ, Eva a Václav BARTÍK. *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.

KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Praha: BOVA POLYGON, 2013. ISBN 978-80-7273-173-2.

KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.

MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1.

NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5.

NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

Ochrana osobních údajů, služební zákon a sociální souvislosti zaměstnávání cizinců. *Sborník příspěvků z mezinárodní vědecké konference*. Brno: Masarykova univerzita, 2018. ISBN 978-80-210-8930-3. Dostupné také z: https://www.law.muni.cz/sborniky/pracpravo2017/files/PracovniPravo2017.pdf

PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): data a soukromí v digitálním světě: komentář*. Praha: Leges, 2018. Komentátor. ISBN 978-80-7502-288-2.

Články a internetové zdroje

Co je GDPR. *Mvcr.cz* [online]. 2017 [cit. 2019-03-17]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

Co je GDPR? *Gdpr.cz* [online]. [cit. 2019-03-17]. Dostupné z: https://www.gdpr.cz/gdpr/

GDPR zasáhne i do zákoníku práce. Na co se musí firmy připravit? *BusinessInfo.cz* [online]. 2018 [cit. 2019-03-17]. Dostupné z: https://www.businessinfo.cz/cs/clanky/gdpr-zasahne-i-do-zakoniku-prace-na-co-se-musi-firmy-pripravit-102429.html

Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z. *Praceamzda.cz* [online]. 2017 [cit. 2019-03-17]. Dostupné z: https://www.praceamzda.cz/clanky/ochrana-osobnich-udaju-zamestnancu-od-pres-gdpr-do-z#footnote3

Péče o zaměstnance a pracovní podmínky. *BusinessInfo.cz* [online]. 2013 [cit. 2019-03-17]. Dostupné z: https://www.businessinfo.cz/cs/clanky/pece-o-zamestnance-a-pracovni-podminky-34157.html#!&chapter=1

Za rok začne být účinná evropská směrnice GDPR. *BusinessInfo.cz* [online]. 2017 [cit. 2019-03-17]. Dostupné z: https://www.businessinfo.cz/cs/clanky/za-rok-zacne-byt-ucinna-evropska-smernice-gdpr-91014.html

Zaměstnavatel a záznamy o činnostech zpracování dle GDPR. *Podnikatel.cz* [online]. 2018 [cit. 2019-03-17]. Dostupné z: https://www.podnikatel.cz/clanky/zamestnavatel-a-zaznamy-o-cinnostech-zpracovani-dle-gdpr/

Zákony

Důvodová zpráva k zákonu č. 101/2000 Sb., o ochraně osobních údajů ze dne 22. 9. 1999

Důvodová zpráva k zákonu č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

Evropská úmluva o ochraně lidských práv

Mezinárodní pakt o občanských a politických právech

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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

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

Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášená pod č. 115/2001 Sb. m. s.

Všeobecná deklarace lidských práv

Zákon č. 1/1993 Sb., Ústava ČR

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

Zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru

Zákon č. 2/1993 Sb., Listina základních práv a svobod

Zákon č. 262/2006 Sb., zákoník práce

Zákon č. 269/1994 Sb., o Rejstříku trestů

Zákon č. 273/2008 Sb., o Policii České republiky

Zákon č. 435/2004 Sb., o zaměstnanosti

Zákon č. 439/2004 Sb., kterým se mění zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

Zákon č. 582/1991 Sb., České národní rady o organizaci a provádění sociálního zabezpečení

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Judikatura

Rozsudek Evropského soudu pro lidská práva ve věci 61496/08 - Bărbulescu proti Rumunsku ze dne 12. 1. 2016 a 5. 9. 2017

Nález Ústavního soudu ČR publikován pod č. 116/2008 Sb., ze dne 12. března 2008 ve věci návrhu na zrušení některých ustanovení zákona č. 262/2006 Sb., zákoník práce

Rozhodnutí Nejvyššího soudu ČR sp. zn. 15 Tdo 574/2006 ze dne 28. 6. 2006

Rozhodnutí Nejvyššího soudu ČR sp. zn. 25 Cdo 4744/2010 ze dne 26. 1. 2012

Rozhodnutí Městského soudu v Praze sp. zn. 7 Ca 204/2005 ze dne 28. 2. 2007

Nález Ústavního soudu ČR sp. zn. I. US 517/10 z dne 15. 11. 2010

Nález pléna Ústavního soudu ČR sp. zn. Pl. ÚS 38/02 ze dne 9. 3. 2004

Nález pléna Ústavního soudu ČR sp. zn. Pl. US 4/94 ze dne 12. 10. 1994

Nález pléna Ústavního soudu ČR sp. zn. Pl. US 40/08 ze dne 26. 5. 2009

Nález pléna Ústavního soudu ČR sp. zn. Pl. US 83/06 ze dne 12. 3. 2008

Stanoviska Úřadu pro ochranu osobních údajů a WP29

Dozorová činnost. *Uoou.cz* [online]. [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/rd=0

K dodržování povinnosti přijmout a provést bezpečností opatření k ochraně osobních údajů v soukromoprávní sféře. *Uoou.cz* [online]. 2013 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/k-dodrzovani-povinnosti-prijmout-a-provest-bezpecnosti-opatreni-k-ochrane-osobnich-udaju-v-soukromopravni-sfere/d-1598/p1=2855

K problémům z praxe – č. 1/2003 – Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců. *Uoouu.cz* [online]. 2003 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/c-1-2003-monitorovani-elektronicke-posty-a-ochrana-soukromi-a-osobnich-udaju-zamestnancu/ds-2551/archiv=0&p1=2515

Stanovisko č. 2/2008 – Souhlas se zpracováním osobních údajů. *Uoou.cz* [online]. 2008 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/files/stanovisko_2008_2.pdf

Pokyny k posouzení vlivu na ochranu osobních údajů a ke stanovení, zda zpracování bude „pravděpodobně mít za následek vysoké riziko. *Uoou.cz* [online]. 2017 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31892

Pokyny týkající se práva na přenositelnost údajů. *Uoou.cz* [online]. 2016 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31882

Sdělení ÚOOÚ k přístupu založenému na riziku. *Uoou.cz* [online]. 2016 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=26872

Stanovisko č. 1/2009 – Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/stanovisko-c-1-2009-zpracovani-osobnich-udaju-na-zaklade-smluv-uzaviranych-se-zpracovateli-tzv-retezeni-zpracovatelu-osobnich-udaju/d-1509

Stanovisko č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/files/stanovisko_2009_2.pdf

Stanovisko č. 4/2012 – Zpracování osobních údajů zemřelých osob. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/files/stanovisko_2012_4_old.pdf

Stanovisko č. 6/2012 – Zpracování osobních údajů zaměstnanců ve vztahu k oznamovací povinnosti správce podle § 16 zákona o ochraně osobních údajů. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/stanovisko-c-6-2012-zpracovani-osobnich-udaju-zamestnancu-ve-vztahu-k-oznamovaci-povinnosti-spravce-podle-16-zakona-o-ochrane-osobnich-udaju/d-1541

Stanovisko Úřadu pro ochranu osobních údajů č. 2/2009 – Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: Dostupné z: https://www.uoou.cz/stanovisko-c-2-2009-ochrana-soukromi-zamestnancu-se-zvlastnim-zretelem-k-monitoringu-pracoviste/d-1511

Stanovisko Úřadu pro ochranu osobních údajů č. 6/2009. Ochrana soukromí při zpracování osobních údajů. *Uoou.cz* [online]. 2009 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/stanovisko-c-6-2009-ochrana-soukromi-pri-zpracovani-osobnich-udaju/d-1519

Z rozhodovací činnosti Úřadu. *Uoou.cz* [online]. [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=5092