ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra pracovního práva a práva sociálního zabezpečení

Diplomová práce

Ochrana osobních údajů v oblasti pracovního práva

Jiří Doljak

Plzeň 2019

„Prohlašuji, že jsem diplomovou práci na téma Ochrana osobních údajů v oblasti pracovního práva zpracoval sám. Veškeré zdroje, kterých bylo užito k sepsání práce, jsem citoval v poznámkách pod čarou a jsou uvedeny v seznamu pramenů v závěrečné části práce.“

V Plzni dne 28. 3. 2019 ……..…..……..…

Jiří Doljak

Tímto bych rád poděkoval vedoucímu mé diplomové práce, panu Mgr. Michalu Dittrichovi, za cenné rady a připomínky, dále bych chtěl poděkovat rodině za podporu při psaní a jmenovitě mé sestře Mgr. Anetě Rozsypalové.

Obsah

1) Úvod

S fenoménem ochrany osobních údajů se v právnickém diskursu České, respektive Československé, republiky setkáváme prakticky již od jejího vzniku, nicméně s ohledem na vstup do Evropské unie a s ním úzce související přijetí unijní legislativy se portfolio právních nařízení působících v oblasti ochrany osobních údajů na našem území rozšiřuje. Nejnovější změnu plynoucí z legislativy Evropské unie v oblasti ochrany osobních údajů pak představuje Obecné nařízení GDPR, které nabylo účinnosti 25. května 2018.

S ohledem na to, jaké obavy aplikaci Nařízení GDPR zejména mezi laickou veřejností provázely, bych se v předkládané diplomové práci rád zaměřil na srovnání zásadních rozdílů mezi českou úpravou ochrany osobních údajů, představovanou zejména Zákonem o ochraně osobních údajů a souvisejícími zákony Zákoníku práce a Zákona o zaměstnanost a úpravou podle Nařízení GDPR, a to nejen z hlediska teoretického (kapitola 7. Významné rozdíly mé práce), ale i z hlediska praktických dopadů na vybrané společnosti (kapitola 8. Vyhodnocení dotazníku). Zatímco v kapitole Významné rozdíly se věnuji zejména srovnání vybraných právních aspektů (osobní údaj, citlivý osobní údaj, fotografie zaměstnance a povinnosti správce a zásady zpracování), jak je definuje na jedné straně Zákon o ochraně osobních údajů a na straně druhé Nařízení GDPR, v následující kapitole Vyhodnocení dotazníku se zaměřuji již na konkrétní prvky, které s sebou zavedení principů Nařízení GDPR přivedlo do praxe jednotlivých společností. V této části práce zhodnotím, jak nákladné (z hlediska finančního, technického i lidských zdrojů) bylo pro jednotlivé firmy přizpůsobení se nové legislativě, zda si změna legislativy vyžádala speciální investice do vzdělávání zaměstnanců či s sebou přinesla požadavky na navýšení počtu pracovníků a v neposlední řadě se zaměřím na cca roční zkušenost s tím, jak se vybrané společnosti na změny přinášené Nařízením GDPR adaptovaly, a zda toto nařízení vnímají pozitivně či zda pro ně z praktického hlediska chodu firmy znamenalo spíše zvýšenou administrativní či ekonomickou zátěž.

V úvodních, teoretických, pasážích textu se věnuji zejména vymezení stěžejních pojmů pro potřeby této diplomové práce, jimiž jsou například termíny:

osobní údaj, citlivý údaj, subjekt údajů, personalistika apod. Hlavními literárními prameny mi pro zpracování této části textu byly zejména příslušné zákony (Zákon o ochraně osobních údajů, Zákon o zaměstnanosti…) a dále pak také odborné monografie renomovaných autorů pracovního práva, mezi jinými například Bartík a Janečková – Ochrana osobních údajů v aplikační praxi.

S ohledem na výše uvedené obavy z prováděných kontrol a sankčních mechanismů plynoucích z Nařízení GDPR jsem se v rámci kapitoly Pojmy podle GDPR zvláště zaměřil právě na tyto dva donucovací prostředky a pokusil se blíže rozpracovat, kdy a za jakých podmínek mohou být aplikovány. Vedle ukotvení příslušných předpisů v Nařízení GDPR mi při psaní této části textu byly oporou i publikace věnující se aplikační problematice GDPR, např. Žůrek – Praktický průvodce GDPR.

V již dříve nastíněné praktické části textu jsem se pak soustředil na porovnání vybraných termínů z hlediska Zákona o ochraně osobních údajů a z hlediska Nařízení GDPR (blíže viz kapitolu Významné rozdíly). Tato kapitola je členěna do čtyř podkapitol, které korespondují se zkoumanými termíny. V rámci každé podkapitoly se pak vždy pokusím shrnout, jaké hlavní rozdíly (pokud zde jsou), je možné sledovat ve vymezení daných pojmů dle Zákona o ochraně osobních údajů a dle Obecného nařízení GDPR.

Poslední a rovněž praktickou kapitolou mé práce je pak komentované vyhodnocení dotazníku mapujícího vliv nového nařízení GDPR na praxi vybraných firem. V rámci elektronického dotazníku, který byl zpracován správci osobních údajů či personalisty daných společností, bylo položeno několik otázek zaměřených na vnímání Nařízení GDPR v soukromém sektoru. Cílem dotazníku bylo zjistit, zda byly firmy nuceny v reakci na zavedení Nařízení GDPR přistoupit k nějakým zásadním změnám ve svém finančním plánu, organizační struktuře či přístupu k osobním údajům zaměstnanců, respektive uchazečů o práci. S ohledem na informace, které v hromadných sdělovacích prostředcích rezonovaly před zavedením Nařízení GDPR, jsem a priori očekával, že hlavní změny firmy pocítí zejména v oblasti nároků na navýšení personálních kapacit (pověřenec pro ochranu osobních údajů - DPO) či požadavků na dodatečné investice do vzdělávání zaměstnanců s přístupem k osobním údajům zaměstnanců. Taktéž

jsem očekával vzrůstající zájem o to, jaké informace zaměstnavatel zpracovává, a to jak ze strany zaměstnanců, tak ze strany uchazečů o zaměstnání.

Cílem mojí práce bude porovnat a zjistit informovanost v jednotlivých firmách a jaký dopad mělo zavedení Nařízení na jejich zpracovávání osobních údajů, citlivých údajů, respektive osobních údajů zvláštní kategorie. Zaměřuji se na změny ve výše zmíněných pojmech, společně pak na změny ohledně fotografií zaměstnanců a úpravu povinností správce a zásad zpracovávání v obou právních předpisech. Další zkoumanou věcí pro mě byl finanční zásah firem po zavedení Nařízení GDPR, ve kterém sektoru byly nuceny udělat největší investici.

2) Vývoj ochrany osobních údajů na území České Republiky

Prvním zákonem, který se zabýval ochranou soukromí byl Zákon č.87/1862 Sb.z.s., o ochraně svobody osobní, a dále pak zákon č.82/1862 Sb.z.s., na ochranu svobody domovní. Po vzniku samostatného Československa byl přijat Ústavní zákon č.293/1920Sb., o ochraně svobody osobní, domovní a tajemství listovního. V následujících letech byl jen mírně upravován v zákonech o držení a vydávání cestovního dokladu a až v 90. letech 20. století se začala kodifikovat úprava ochrany osobních údajů. Nejprve zákonem č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech a následně pak v Listině základních lidských práv a svobod, vyhlášená Usnesením předsednictva České národní rady č.2/1993 Sb. Až v roce 2000 byl vyhlášen Zákon č. 101/2000 Sb, o ochraně osobních údajů, který platí dodnes. V prosinci roku 2009 vstoupila v platnost Lisabonská smlouva, která novelizovala Smlouvu o Evropské unii. V rámci novelizace došlo k povýšení Listiny Základních práv Evropské unie na roveň Lisabonské smlouvy, byla jí tím přiznána stejná právní síla jako Lisabonské smlouvě, čímž se Listina de facto stala její součástí.[1]

Článek 8 Listiny základních práv EU

Ochrana osobních údajů

1. *Každý má právo na ochranu osobních údajů, které se ho týkají.*
2. *Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.*
3. *Na dodržování těchto pravidel dohlíží nezávislý orgán.*[2]

Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů byl přijat na základě Směrnice Evropského parlamentu a rady 95/46/es o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a na

[1] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 28
[2] Listina základních práv Evropské unie článek 8

základě Úmluvy Rady Evropy č. 108, o ochraně se zřetelem na automatizované zpracování osobních údajů. V zákoně jsou upraveny práva a povinnosti týkající se zpracování osobních údajů. Zahrnuje soukromoprávní problematiku a v případě Úřadu na ochranu osobních údajů také veřejnoprávní problematiku.

„*Naplnění osobní potřeby je svojí povahou specifickým účelem zpracování osobních údajů a jako takové musí být legální a legitimní. Za osobní potřebu, tak nelze považovat zpracování osobních údajů v souvislosti s trestnou činností fyzické osoby (např. pro účely vydírání, nebo stalkingu) nebo zpracování osobních údajů získaných neoprávněně, protiprávně, např. krádeží dat z informačního systému jiného subjektu.“*[3]

Nařízení GDPR a česká legislativa

Do vstupu platnosti Obecného nařízení o ochraně osobních údajů, byla ochrana osobních údajů v České republice řešena Zákonem o ochraně osobních údajů, který upravoval mimo jiné i funkci dozorčího úřadu, který u nás reprezentuje Úřad pro ochranu osobních údajů. Odborníci tento právní předpis hodnotili kladně, nicméně v různých členských státech bylo dosahování cílů směrnice odlišné. Rozdíly v ochraně osobních údajů, v různých členských státech Evropské unie, by tak v konečném důsledku mohly bránit nejen volnému pohybu osobních údajů v rámci Unie, ale také mohou narušit hospodářské činnosti či soutěž na úrovni Evropské unie.[4]

„Úroveň ochrany osobních údajů musí být ve všech členských státech Evropské unie stejná. Jednotlivé členské státy, si pak mohou přijmout konkrétnější ustanovení, včetně zvláštních pravidel na zpracování zvláštní kategorie osobních údajů. GDPR proto nevylučuje zpřesnění určení podmínek, za kterých je zpracování osobních údajů ještě zákonné“[5].

„*Účinná ochrana osobních údajů v celé Evropské unii vyžaduje také rovnocenné sankce za jejich porušení v členských státech a vyžaduje spolupráci dozorových úřadů v jednotlivých členských státech. GDPR by nemělo příliš*

3 Kučerová, A., Nováková, L., Foldová V., Nonnemann, F., Pospíšil, D., Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2012, str. 19

4 NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 67

5 NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 67

administrativně zatěžovat podniky, které mají méně než 250 zaměstnanců, ty mají velké úlevy a na to by měly reagovat i členské státy ve své legislativě.“[6]

[6] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 67

3) Pojmy dle Zákona o ochraně osobních údajů

Osobní údaj

„Osobními údaji 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.“[7]

Citlivý údaj

„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 nebo autentizaci subjektu údajů,“[8]

Subjekt údajů

„Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.“[9]

Zpracování osobních údajů

„Zpracováním osobních údajů se rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření,

[7] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno a)
[8] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno b)
[9] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno d)

zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.“[10]

Shromažďování osobních údajů

„Shromažďování osobních údajů je systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.“[11]

Uchování osobních údajů

„Uchovávání osobních údajů znamená udržování údajů v takové podobě, která je umožňuje dále zpracovávat.“[12]

Likvidace osobních údajů

„Likvidací je myšleno fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.“[13]

Správce osobních údajů

„Správcem osobních údajů je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí jejich zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“[14]

[10] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno e)
[11] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno f)
[12] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno g)
[13] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno i)
[14] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno j)

Zpracovatel osobních údajů

„Zpracovatelem se rozumí každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.“[15]

Zveřejněný osobní údaj

„Zveřejněným osobním údajem je osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.“[16]

Evidence nebo soubor datový soubor osobních údajů

„Evidencí nebo datovým souborem osobních údajů (dále jen "datový soubor") je jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.“[17]

Souhlas subjektu údajů

„Souhlasem subjektu údajů je svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“.[18]

Příjemce

„Příjemcem se rozumí každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje dle §3 odstavec 6 písmeno g) Zákon o ochraně osobních údajů.“[19]

[15] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno k)
[16] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno l)
[17] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno m)
[18] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno n)
[19] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písmeno o)

Personalistika

„Personalistika bývá obecně charakterizována jako činnost, která se zaměřuje na získávání pracovníků a práci s nimi. V širším slova smyslu je pak činností, kterou vykonává každý zaměstnavatel, který má či hodlá mít zaměstnance, a zahrnuje v sobě zejména plnění zákonných povinností, jež zaměstnavatelům ukládají zvláštní právní předpisy, ale také činnosti, které jsou v zájmu samotného zaměstnavatele na základě jeho vlastního rozhodnutí a týkají se jeho zaměstnanců. Vzhledem k tomu, že není myslitelné, aby se personální práce obešla bez údajů osob (zaměstnanců) jichž se personální práce týká, bude se na činnosti personalistiky vztahovat také Zákon o ochraně osobních údajů. Rozdíl bude jen v tom, v jakém režimu, respektive jaká ustanovení Zákona o ochraně osobních údajů, budou dotčena a jaká práva a jaké povinnosti budou stíhat zaměstnavatele, a tedy, jakými ustanoveními uvedeného zákona se budou jednotlivá zpracování řídit.“[20]

Václav Bartík s Evou Janečkovou ve své publikaci Ochrana osobních údajů v aplikační praxi uvádějí tři základní části zpracování osobních údajů, kterými jsou zpracování před uzavřením pracovního nebo obdobného poměru, zpracování v jeho průběhu a po jeho skončení.[21]

Zpracování osobních údajů před uzavřením pracovního poměru

„Základní právní úprava mezi fyzickou osobou a potenciálním zaměstnavatelem z hlediska pracovního práva představuje Zákon č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů a Zákoník práce. Pracovní vztahy nebyly nijak upraveny do přijetí Zákona o zaměstnanosti, a to činilo aplikační problémy z hlediska ochrany a zpracování osobních údajů. Kvůli absenci právní úpravy činily největší problém záležitosti týkající se rozsahu osobních údajů, které potencionální zaměstnavatel po uchazečích vyžadoval, stejně tak údaje, které poskytovaly personální agentury, zejména pokud tyto agentury byly správci osobních údajů, jimiž byly, pokud samy aktivně působily na trhu práce. Vždy když

[20] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 153

[21] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. S. 153

agentury shromažďovaly osobní údaje uchazečů o práci bez zakázky konkrétního zaměstnavatele.[22]“

Problém vidí Václav Bartík a Eva Janečková zejména v aplikaci ustanovení §5 odst. 1 písmeno d) Zákona o ochraně osobních údajů[23], v němž je uvedeno, že: „*Správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,“.*[24] Podle obou autorů je totiž účel definován vágně a jeho formulace tak umožňovala pracovním agenturám shromažďovat množství informací o registrovaných uchazečích o práci, o to i informací takového typu, které nebyly pro nalezení vhodné práce relevantní (například informace o majetkových poměrech klientů, rodinných vztazích či dokonce o plánovaných sňatcích anebo zamýšleném počtu dětí).

Tehdy platné znění Zákona o ochraně osobních údajů tuto praxi do jisté míry umožňovalo, když v. Ustanovení §5 odstavec 4 Zákona o ochraně osobních údajů v tehdy platném znění (do 25. 4. 2004) uvádělo, že „*… ze souhlasu musí být patrné, v jakém rozsahu je poskytován, komu a k jakému účelu, na jaké období a kdo jej poskytuje. Souhlas může být kdykoliv odvolán, pokud se subjekt údajů se správcem výslovně nedohodne jinak. Tento souhlas musí správce prokázat po dobu zpracování údajů, k jejichž zpracování byl dán souhlas.“*[25] Takovým souhlasem personální agentury jistě disponovaly, i když se vedly spory o „dobrovolnosti“ udělení tohoto souhlasu.[26]

Tento problém s kvalitou souhlasu řeší podle Bartíka a Janečkové nová definice uvedená v novele Zákona o ochraně osobních údajů Zákonem č. 439/2004 Sb., kterou najdeme v ustanovení §4 písmeno n) Zákona o ochraně osobních údajů[27]: *„souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů,“*[28]. Dále tato novela definovala další parametry souhlasu v ustanovení

---

22 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. S. 153

23 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. S. 153

24 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(1) písm. d)

25 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(4) v tehdejším znění

26 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 154

27 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 154

28 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písm. n)

§5 odstavec 4: „*Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.*“[29] Souhlas se zpracováním osobních údajů je tedy jednoznačně jednostranné právní jednaní, zcela v souladu s ustanovením §545 a následující Občanského zákona, a tak je třeba jej vykládat a aplikovat.[30]

Z hlediska ochrany osobních údajů byly limity toho, co může zaměstnavatel požadovat před zahájením výběrového řízení po uchazečích, stanoveny Zákonem o zaměstnanosti (viz níže): „*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, 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. Ustanovení § 4 platí i zde*.“[31]

Platí také, že zaměstnavatel by tak neměl zjišťovat citlivé údaje o uchazečích, avšak jsou výjimky, kdy je to pro zaměstnavatele potřebné. Kupříkladu, pokud je na danou pracovní pozici stanoven zvláštním právním předpisem požadavek bezúhonnosti či pokud daná práce klade nároky na zdraví a kondici zaměstnance, za jejichž naplnění s ohledem na ochranu zdraví pracovníka je zaměstnavatel odpovědný.[32] Na druhou stranu ale, pokud by zaměstnavatel požadoval informace bez přímé opory ve zvláštním právním předpisu, mohl by se svým jednáním dostat do rozporu s §5 odstavec 1 písmeno d) Zákona o ochraně osobních údajů, dle něhož je zaměstnavatel oprávněn „s*hromažďovat osobní údaje*

29 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(4)
30 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 154
31 Zákon č.435/2004Sb., Zákon o zaměstnanosti; §12(2)
32 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 155

odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,"[33]

Zákoník práce před novelizováním neobsahoval žádnou úpravu prepracovních vztahů; jediné limity pro zaměstnavatele týkající se ochrany osobních údajů tak poskytovaly Zákon o zaměstnanosti společně se Zákonem na ochranu osobních údajů. Na druhou stranu současný Zákoník práce věnuje postupu zaměstnavatelů a zpracování osobních údajů uchazečů před vznikem pracovního poměru pozornost, když v §30 stanoví[34]:

„*(1) Výběr fyzických osob ucházejících se o zaměstnání z hlediska kvalifikace, nezbytných požadavků nebo zvláštních schopností je v působnosti zaměstnavatele, nevyplývá-li ze zvláštního právního předpisu jiný postup; předpoklady kladené zvláštními právními předpisy na fyzickou osobu jako zaměstnance tím nejsou dotčeny.*

(2) 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."[35]

V tomto případě hovoříme o základních identifikačních údajích, tedy jménu (či jménech) a příjmení uchazeče, adrese bydliště a datu narození, dále pak o kontaktních údajích (zpravidla emailová adrese a číslo telefonu) a pak také o informacích týkajících se vzdělání uchazeče, praxe v oboru a případně dalších předpokladech a schopnostech vztahujících se k obsazované pracovní pozici.[36]

Vedle Zákoníku práce jsou nadále platné limity stanovené Zákonem o zaměstnanosti a Zákonem o ochraně osobních údajů. Pokud bude zaměstnavatel respektovat a plnit nařízení všech tří výše uvedených právních předpisů, měl by dosáhnout na jedené straně dostatečné ochrany osobních údajů svých zaměstnanců a na straně druhé také by měl mít k dispozici i dostatek relevantních informací pro svoji personální činnost a výběr vhodných uchazečů na požadovanou pracovní pozici.

---

[33] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(1) d)

[34] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 155

35 Zákon č.262/2006 Sb., Zákoník práce; §30

[36] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 155

V rámci postupu zaměstnavatele před vznikem pracovního poměru dochází k systematickému zpracování osobních údajů uchazečů a je třeba odpovědět si otázku, zda k tomuto zpracování zaměstnavatel, tedy správce, osobních údajů, potřebuje souhlas subjektu údajů, nebo tak může činit bez jeho souhlasu. Odpověď nalezneme v §5 odstavec 2 Zákona o ochraně osobních údajů, v jeho návětí: „Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,"[37] *a dále pak v písmenu b téhož paragrafu téhož zákona: „jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,"*[38] *V případě náboru zaměstnanců se jedná právě o tento případ. Obecně bývá pravidlem, že zaměstnavatel, hledající novou pracovní sílu, dá tuto skutečnost najevo veřejným sdělením, nejčastěji se jedná o nabídkové inzeráty na specializovaných internetových stránkách, popřípadě v denním tisku. Zveřejňovány nejčastěji bývají jen základní požadavky na dané pracovní místo a od uchazeče je požadován strukturovaný životopis a sdělení kvalifikačních předpokladů, přičemž je ponecháno na uchazeči, jaké údaje o sobě v požadovaných dokumentech skutečně uvede.*[39]

Výsledkem tak nakonec je rozsáhlá databáze tvořená dokumenty od jednotlivých uchazečů, která obsahuje osobní údaje každého jednoho z nich, ač vnitřní struktura jednotlivých dokumentů je zpravidla různá, ačkoliv bývá velmi obdobná. Tento soubor osobních údajů všech uchazečů o zaměstnání splňuje náležitosti dle definice §4 písmeno m) zákona o ochraně osobních údajů: „evidencí nebo datovým souborem osobních údajů (dále jen "datový soubor") jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií,[40] *a je evidencí, která je dále zpracována za účelem výběru nejvhodnějšího uchazeče, přičemž konečným cílem a účelem zpracování je uzavření pracovní smlouvy s vybraným kandidátem. Je tedy zřejmé, že je splněno ustanovení z §5 odstavec 2 písmeno b) Zákona o ochraně osobních údajů: „jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na*

37 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (2) návětí
38 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (2) písm. b)
39 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 156
40 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písm. m)

návrh subjektu údajů,"[41] *protože se jedná o jednání o uzavření smlouvy, byť je toto jednání pouze v zahajovacím stadiu. Není tedy potřeba, aby zaměstnavatel zpracovával tyto údaje s formalizovaným souhlasem subjektů údajů, v tomto případě uchazečů o zaměstnání. Je zřejmé, že uchazeči jsou obeznámeni s účelem (prostřednictvím zveřejňování informací), k němuž poskytují své osobní informace, a komu. Znají rozsah údajů, neboť na základě rámcové informace poskytují sami o své vůli a v rozsahu velmi často i větším, než je požadováno. Mohou do značné míry také dovodit, na jak dlouhou dobu je poskytují (do doby než je vybrán vhodný uchazeč), a jsou s těmito informacemi srozuměni.*[42]

Současně to však neznamená, že je zaměstnavatel zbaven povinností plnit další ustanovení Zákona o ochraně osobních údajů. To znamená, že tyto zpracované osobní údaje musí především chránit před zneužitím, jak stanovuje §13 Zákona o ochraně osobních údajů:

„(1) *Správce a zpracovatel jsou povinni 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. Tato povinnost platí i po ukončení zpracování osobních údajů.*

(2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

(3) V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se:

a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,

b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,

c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a

41 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (2) písm. b)

42 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 156

d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

(4) V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také

a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,

b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,

c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a

d) zabránit neoprávněnému přístupu k datovým nosičům, "[43]

a může je použít jen k účelu, k němuž byly shromážděny, a to po dobu nezbytně nutnou k dosažení stanoveného účelu. V praxi to znamená, že jakmile je vybrán vhodný uchazeč a je s ním uzavřena smlouva, tak pominul důvod, pro který byly shromážděny osobní údaje všech ostatních uchazečů. Tímto také končí oprávnění zaměstnavatele dále zpracovávat tyto osobní údaje bez souhlasu subjektu údajů, tedy si je ponechat pro možné pozdější využití, neboť jiná z ostatních výjimek v ustanovení §5 odstavec 2 Zákona o ochraně osobních údajů není aplikovatelná.: „Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,

c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu

43 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §13

získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,

d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,

e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,

f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo,

g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona."[44]

Správce není oprávněn osobní údaje uchovávat či jinak zpracovávat poté, co pomine účel jejich shromáždění. To znamená, že bezprostředně po ukončení výběrového řízení by měl zaměstnavatel zlikvidovat všechny přihlášky a související podklady od uchazečů, kteří ve výběrovém řízení nebyli úspěšní, a to bez ohledu na to, zda byli pozváni k osobnímu pohovoru, či nikoliv, popřípadě je vrátit.[45]

Pokud však si chce zaměstnavatel ponechat tyto nabídky pro potřeby dalšího využití, může tak učinit pouze se souhlasem dotčených osob. Takový souhlas pak musí splňovat podmínky, které pro tento úkon stanoví §4 písmeno n)[46] ve spojení s §5 odstavcem 4 Zákona o ochraně osobních údajů.:

„*Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na*

44 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (2)

[45] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 2016-04-10]. ISBN 978-80-210-6819-3. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

[46] Viz kapitola pojmy

jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.“[47]

„*Účel tohoto využití pak musí být nově stanoven, na příklad jako databáze potencionálních zaměstnanců, kteří sice obecně splňují předpoklady pracovního uplatnění, ale v daném okamžiku pro ně není volné pracovní místo, které se ovšem v budoucnu uvolnit může. Na takové zpracování pak dopadají všechna ustanovení Zákona o ochraně osobních údajů, tedy zejména základní povinnosti v §5 odstavec 1*“[48]:

„*Správce je povinen*

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) stanovit prostředky a způsob zpracování osobních údajů,

c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6.) Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům,

d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,

e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné,

f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích

47 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (4)

[48]BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 157

ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

h) nesdružovat osobní údaje, které byly získány k rozdílným účelům."[49]

Přiměřenou dobou uchování osobních údajů v databázi potencionálních zaměstnanců pak Václav Bartík odhaduje zhruba na 6 měsíců. Podle něj lze předpokládat, že za půl roku se již na straně uchazeče mohou změnit okolnosti natolik, že evidování těchto údajů ztrácí pro zaměstnavatele smysl. Opět zde platí, že po uvedené době nebude mít zaměstnavatel právo disponovat těmito údaji, tedy je zpracovávat, a bude povinen je zlikvidovat, pokud se se subjektem nedohodnou jinak, což v praxi znamená vrácení údajů subjektu.[50]

„*Žádný právní předpis neukládá zaměstnavatelům, aby zřizovali a vedli evidenci potencionálních pracovníků, bude se na zpracování osobních údajů potencionálních zaměstnanců vztahovat oznamovací povinnost podle §16 Zákona o ochraně osobních údajů.*"

Zpracování osobních údajů za trvání pracovního poměru

Uzavřením pracovní smlouvy zakládá zaměstnavatel zaměstnanci takzvaný osobní spis. V něm jsou zahrnuty dokumenty potřebné pro uzavření a plnění pracovní smlouvy, které mohou obsahovat také osobní údaje zaměstnanců, například doklad o dosaženém vzdělání či údaje z občanského průkazu nebo řidičského oprávnění. V osobním spise by měly být zahrnuty pouze informace o pracovním vztahu. Avšak mohou vzniknout situace, kdy zaměstnavatel potřebuje informace nad rámec práce vykonávané zaměstnancem. Tyto informace sděluje zaměstnanec sám, aby zaměstnavatel mohl dostát svým povinnostem. Příkladem může být účast ve zvláštních sociálních programech, potřebovat volna na vyřízení soukromých záležitostí nebo povinností (svatba,

49 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(1)

50 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 157

narození dítěte, darování krve, úmrtí příbuzného, jednání u soudu) či zapojení se do benefitních programů zaměstnavatele.[51]

Přesné informace o přístupu a nakládání s osobním spisem můžeme nalézt v §312 Zákoníku práce:

„(1) Zaměstnavatel je oprávněn vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3.

(2) Do osobního spisu mohou nahlížet vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, Úřad práce České republiky, Úřad pro ochranu osobních údajů, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby. Za nahlížení do osobního spisu se nepovažuje předložení jednotlivé písemnosti zaměstnavatelem z tohoto spisu vnějšímu kontrolnímu orgánu, který provádí kontrolu u zaměstnavatele a který si tuto písemnost vyžádal v souvislosti s předmětem kontroly prováděné u zaměstnavatele.

(3) Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele“[52].

Zpracování osobních údajů ve vztahu k oznamovací povinnosti správce je popsáno podle § 16 Zákona o ochraně osobních údajů následovně:

„(1) Ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováváním osobních údajů.

(2) Oznámení musí obsahovat tyto informace:

a) identifikační údaje správce, u fyzické osoby, která není podnikatelem, jméno, popřípadě jména, příjmení, datum narození a adresu místa trvalého pobytu, u jiných subjektů obchodní firmu nebo název, sídlo a identifikační číslo osoby, pokud bylo přiděleno,

[51] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

[52] Zákon č.262/2006 Sb., Zákoník práce; §312

a jméno, popřípadě jména, a příjmení osob, které jsou jejich statutárními zástupci,

b) účel nebo účely zpracování,

c) kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají,

d) zdroje osobních údajů,

e) popis způsobu zpracování osobních údajů,

f) místo nebo místa zpracování osobních údajů,

g) příjemce nebo kategorie příjemců,

h) předpokládaná předání osobních údajů do jiných států,

i) popis opatření k zajištění ochrany osobních údajů podle § 13.

(3) Obsahuje-li oznámení všechny náležitosti podle odstavce 2 a není-li zahájeno řízení podle § 17 odst. 1, lze po uplynutí lhůty 30 dnů ode dne doručení oznámení zahájit zpracování osobních údajů. Úřad v takovém případě zapíše informace uvedené v oznámení do registru.

(4) Neobsahuje-li oznámení všechny náležitosti podle odstavce 2, Úřad neprodleně zašle oznamovateli výzvu, v níž upozorní na chybějící nebo nedostatečné informace a stanoví lhůtu k doplnění oznámení. V případě doplnění oznámení začíná běžet lhůta podle odstavce 3 dnem doručení doplnění oznámení. V případě, že Úřad neobdrží doplnění oznámení ve stanovené lhůtě, nahlíží na učiněné oznámení tak, jako by nebylo podáno.

(5) O provedení registrace vydá Úřad na žádost správce osvědčení, které obsahuje datum vyhotovení, číslo jednací, jméno, příjmení a podpis osoby, která osvědčení vydala, otisk úředního razítka, identifikační údaje správce a účel zpracování.

(6) Je-li podle odstavce 1 oznámeno zpracování, které je předmětem kontroly, Úřad registraci neprovede. Úřad registraci provede, jakmile je kontrola ukončena."[53]

Podle ustanovení v §16 Zákona o ochraně osobních údajů, je každý správce a zpracovatel osobních údajů povinen se registrovat u Úřadu pro ochranu osobních údajů. Výjimky tvoří příklady uvedené v §18 odstavec 1 Zákona na ochranu osobních údajů, oznamovací povinnost se na správce nevztahuje, pokud

53 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §16

mu povinnosti správce stanovuje zvláštní zákon, nebo jsou takové osobní údaje nutné k uplatnění práv a povinností vyplývajících ze zvláštního zákona, osobní údaje jsou součástí veřejně přístupných datových souborů nebo jde o zpracování sledující politické, filosofické apod. cíle prováděné v rámci oprávněné činnosti sdružení, které se týká pouze jeho členů, a údaje nejsou přístupné bez souhlasu subjektů.[54]

„Znamená to tedy, že správce osobních údajů – zaměstnavatel – musí znát a aplikovat řadu právních předpisů, které mu ukládají mnoho povinností a z nichž plyne, že musí zpracovávat značné množství osobních údajů zaměstnanců. Kromě základního předpisu pracovního práva, kterým je Zákoník práce, musíme poukázat i na zákon č.48/1997 SB., o veřejném zdravotním pojištění, zákon č. 155/1995Sb., o důchodovém pojištění.[55]

Pokud správci údajů nestanovuje zvláštní předpis jinak, bude se zpracování řídit obecným pravidlem v ustanovení §5 odstavce 1 Zákona o ochraně osobních údajů. K takovému zpracování takových údajů je vyžadován souhlas zaměstnance. Příkladem je sociální program, který umožňuje zaměstnancům čerpat nějaké benefity pro rodinné příslušníky. Někteří správci si zjednodušují práci a chtějí po zaměstnancích kopii rodného listu, Zřídkakdy pak zaměstnanec takovýto požadavek odmítne, a to vede k založení všech informací do spisu, i když neobsahují nic s poskytovanou výhodou. To pak vede k uchování a zpracovávání osobních údajů osob, u kterých k tomu zaměstnavatel nemá oprávnění.[56]

Na zpracování osobních údajů zaměstnanců za účelem vedení mzdové a personální agendy, pro dodržení povinností, které mu stanovuje zvláštní právní předpis, se oznamovací povinnost podle ustanovení §16 Zákona o ochraně osobních údajů nevztahuje. Toto ustanovení stanovuje oznamovací povinnost pro zaměstnavatele, pokud osobní údaje zpracovává za jiným účelem, než mu stanovuje zvláštní zákon, nebo z žádného nevyplývají. Zpracování těchto osobních údajů je založeno na souhlasu subjektů údajů.[57]

---

54 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §18

55 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 158

56 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 159

57 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 159

Zpracování citlivých osobních údajů v pracovně-právním poměru

„Citlivé osobní údaje jsou zvláštním druhem osobních údajů, které mohou samy o sobě poškodit subjekt údajů ve společnosti a mohou vést až k diskriminaci fyzické osoby.“[58] Směrnice 95/46/ES tuto kategorii osobních údajů definuje ve svém v článku 8, definuje jako takzvanou: „*zvláštní kategorii osobních údajů, což jsou takové údaje, které odhalují rasový či etnický původ, náboženské vyznání, politické názory, filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se jejich zdraví a sexuálního života*.“[59]

Zákon o ochraně osobních údajů v ustanovení §4 písmeno b) je definuje takto:

„*citlivým údajem 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 nebo autentizaci subjektu údajů*,“[60].

Regulaci zpracování citlivých údajů nalezneme v Zákoně o ochraně osobních údajů v §9 a konkrétně v písmeni d):

„*je zpracování nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem*.“[61]

Zvláštním zákonem se v tomto případě myslí hlavně Zákoník práce a jeho ustanovení §316 odstavec 4:

„*Zaměstnavatel nesmí vyžadovat od zaměstnance informace, které bezprostředně nesouvisejí s výkonem práce a se základním pracovněprávním vztahem uvedeným v §3. Nesmí vyžadovat informace zejména o*

---

[58] Úřad pro ochranu osobních údajů. Zvláštní kategorie osobních údajů (citlivé údaje). [online] 5. 3. 2018 [cit. 20. 3. 2019]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaju-citlive-udaje/d-27274/p1=4744

59 Směrnice 95/46/ES článek 8 nadvětí a odstavec 1

60 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 psím b)

61 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §9 písm. d)

a) těhotenství,

b) rodinných a majetkových poměrech,

c) sexuální orientaci,

d) původu,

e) členství v odborové organizaci,

f) členství v politických stranách nebo hnutích,

g) příslušnosti k církvi nebo náboženské společnosti,

h) trestněprávní bezúhonnosti;

to, s výjimkou písmen c), d), e), f) a g), neplatí, jestliže je pro to dán věcný důvod spočívající v povaze práce, která má být vykonávána, a je-li tento požadavek přiměřený, nebo v případech, kdy to stanoví tento zákon nebo zvláštní právní předpis. Tyto informace nesmí zaměstnavatel získávat ani prostřednictvím třetích osob. [62]

Z tohoto jasně vyplývá, že Zákoník práce připouští možnost otázek ohledně těhotenství, trestní bezúhonnosti, majetkových poměrů, pokud je to přímo nezbytné k výkonu činnosti. Například těhotná žena nemůže vykonávat těžké práce či noční směny, nebo pravomocně odsouzený nemůže pracovat na místech s vyššími nároky na bezpečnost (policie apod.). Dalším důvodem, kdy může zaměstnavatel tyto informace vyžadovat, je, pokud mu to přímo stanoví zákon, nebo jiný právní předpis. Příkladem mohou být státní úředníci, u kterých je bezúhonnost vyžadována Služebním zákonem.

Zákoník práce některé citlivé údaje přímo taxativně vymezuje v ustanovení, které jsem uvedl výše, ale je vždy nezbytné posoudit obecnou úpravu podle Zákona o ochraně osobních údajů a zejména limit stanovený v §5 odstavec 1 písmeno d)[63]*:*

„*shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu*,“[64]

62 Zákon č.262/2006 Sb., Zákoník práce; §316 (4)

63 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 163

64 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (1) písm. d)

Dále samozřejmě platí, že pokud zaměstnavatele zákon přímo nestanoví zpracování citlivých údajů, může tak činit pouze se souhlasem zaměstnance. Tento souhlas musí splňovat všechny náležitosti ustanovené v §9 písmeno a)[65]:

„*subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle § 12 a 21*“. [66]

Jak vyplývá z tohoto ustanovení, tak zaměstnavatel nemůže shromažďovat informace o sexuální orientaci, původu, členství v odborových organizacích, členství v politických stranách a hnutích a příslušnosti k libovolné církvi, byť by k tomu dal zaměstnanec souhlas, protože tyto citlivé údaje jsou absolutně vyňaté z diskrece zaměstnavatele z důvodu uvedeného v ustanovení §316 odstavci 4 Zákoníku práce, který jasně zakazuje zaměstnavatele tyto informace vyžadovat, a to znamená, že jimi nemůže jakkoliv disponovat.[67]

Zdravotní stav

Jedná se o jeden z nejvíc problémových pohledů zaměstnavatele, který si často myslí, že zpracovává citlivé údaje o zaměstnanci, i když tomu tak ve skutečnosti není, jelikož zaměstnavatel musí vědět, jestli zaměstnanec je schopen vykonávat danou práci. Údaje, které jsou považovány za citlivé a nemají vliv na výkon zaměstnání, může zpracovávat pouze smluvní závodní lékař nikoliv zaměstnavatel. Zákoník práce předepisuje zaměstnavatelům shromažďovat údaje, někdy i citlivé, o zdravotním stavu zaměstnanců. Podle ustanovení §105 odstavec 2 Zákoníku práce[68]:

---

65 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 163

66 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §9 písm. a)

67 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 164

68 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 165

„Zaměstnavatel je povinen vést v knize úrazů evidenci o všech úrazech, i když jimi nebyla způsobena pracovní neschopnost nebo byla způsobena pracovní neschopnost nepřesahující 3 kalendářní dny.“ [69]

Výpis z rejstříku trestů

Mezi citlivé údaje nepatří informace o trestním stíhání (ctíme presumpci neviny) ani prostá informace o tom, že dotčená osoba nemá záznam v rejstříku trestů. Takové informace jsou ale osobním údajem ve smyslu §4 písmeno a) Zákona o ochraně osobních údajů.[70]

Údaje, které vypovídají o trestné činnosti, jsou údaje o osobách pravomocně odsouzených soudy České republiky, kterým jsou založeny záznamy z trestních listů podle §3 odstavec 3 zákona č.269/1994 Sb., o Rejstříku trestů, které obsahují údaje o:

a) *osobě odsouzeného, aby nebyl zaměnitelný s jinou osobou*
b) *soudu, spisové značce trestní věci*
c) *rozhodnutí o vině, trestu a ochranném opatření a o jejich výkonu*
d) *rozhodnutí soudu při podmíněném odsouzení nebo podmíněném propuštění z výkonu trestu nebo upuštění od zbytku výkonu trestu*
e) *udělení milosti*
f) *účasti odsouzeného na amnestii*
g) *zahlazení odsouzení*[71]

V ustanovení §3 a §4 Zákona o rejstříku trestů, se do evidence zaznamenávají i údaje o odsouzení cizozemským soudem, pokud o jeho uznání rozhodl Nejvyšší soud. Údaji vypovídajícími o trestné činnosti jsou pak také údaje uváděné v opisech a výpisech z rejstříku trestů. V §10 odstavec 5 Zákona o Rejstříku trestů je stanoveno, že[72]: *„v opisu se uvádějí všechny údaje o každém odsouzení osoby, které se opis týká, a všechny údaje o průběhu výkonu trestů a ochranných opatření i o zahlazení odsouzení“*.[73]

69 Zákon č.262/2006 Sb., Zákoník práce; §105 (2)
[70] Viz pojmy
71 BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 166
[72] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 167
73 Zákon č. 269/1994 Sb., Zákon o rejstříku trestů; §10 (5)

Ustanovení §11 až §13 upravují vydání výpisu na písemnou žádost osoby. V něm budou uvedena všechna nezahlazená odsouzení včetně údajů o průběhu výkonu uložených trestů a ochranných opatření, pokud se dle zákona na pachatele nehledí, jako by nebyl odsouzen. To lze považovat za dostatečně úplné vymezení údajů vypovídajících o trestné činnosti.[74]

Zákon o zaměstnanosti stanovil pro údaje o trestné činnosti, které jsou z pohledu Zákona o ochraně osobních údajů, speciální režim, a to, že tyto údaje jsou potřebné. Zaměstnavatel však není vždy oprávněn tyto informace získávat.

Faktem je, že nepřijetí uchazeče o zaměstnání výhradně z důvodu odsouzení za trestnou činnost může v některých případech být porušením právní povinnosti zaměstnavatele. V případě záznamu v Rejstříku trestů, zaměstnavatel musí poměřit závažnost trestného činu s charakterem práce. Například odmítnutí uchazeče se záznamem za majetkovou trestnou činnost na pozici bankéře je na místě, pokud by se však jednalo o práci uklízeče tak už nikoliv[75].

Zaměstnavatel, jako správce údajů, musí stanovit účel, ke kterému mají být osobní údaje zpracovány, a následně je zpracovat v rozsahu nezbytném pro jeho naplnění. Pokud tak nepostupuje, porušuje Zákon o ochraně osobních údajů, stejně tak i Listinu základních práv a svobod a to v článku 10 odstavci 3, který každému zaručuje právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobnosti.[76] Pokud není zaměstnavatel schopen odůvodnit potřebu získání a zpracování údaje o bezúhonnosti, dopouští se porušení ustanovení §5 odstavec 1 písmeno a) Zákona o ochraně osobních údajů, který mu jasně dává povinnost stanovit účel, k němuž mají být osobní údaje zpracovány.[77] V tomto případě by se jednalo o správní delikt, který rozhoduje Úřad pro ochranu osobních údajů a může stanovit pokutu.[78]

---

[74] DOLEČEK Marek. Ochrana osobních údajů – citlivé údaje. [online] 6. 2018 [cit. 23. 3. 2019] dostupná z: https://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-ppbi-51068.html#!&chapter=4

[75] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 167

76 Listina základních práv a svobod; Článek 10 odstavec 3

77 Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 odstavec 1 písm. a)

[78] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 167-168

Národnost

S integrací do Evropské unie, která přinesla propojení pracovních trhů, se stala aktuální problematika zaměstnávání cizinců, a tím tedy i zpracování citlivých osobních údajů o národnosti, respektive stání příslušnosti zaměstnanců. Cizí státní příslušníci, kteří dlouhodobě pobývají na našem území, většinou z pracovních důvodů, mají povolení k pobytu, které obsahuje informaci o státní příslušnosti. Čili se nejedná o citlivý údaj o národnostním původu, kterým, pokud ho zaměstnavatel vyžaduje, se dopouští porušení Zákona na ochranu osobních údajů, protože není zákonný důvod k jeho zpracování. Naopak informaci o státní příslušnosti zaměstnavatel potřebuje vědět, protože mu to ukládají speciální zákony jako například Zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění.[79]

Fotografie v osobním spise zaměstnance z hlediska zákona o ochraně osobních údajů

„*Často bývá jednou ze součástí osobního spisu zaměstnance jeho fotografie. Důvodů, proč zaměstnavatel vyžaduje fotografii je mnoho, v praxi bývá nejčastěji uváděn důvod bezpečnostní. Dalším důvodem je pak umístění fotky na intranet. Když zaměstnavatel hodlá použít fotografii zaměstnance, musí vzít v potaz Zákon o ochraně osobních údajů.*“[80]

Z fotografie, samozřejmě v závislosti na její kvalitě, se dá subjekt údajů identifikovat. Jsou-li tyto fotografie systematicky zpracovávány, jedná se o zpracování osobních údajů ve smyslu Zákona o ochraně osobních údajů. Častým dotazem bývá, jestli se jedná o zpracování citlivých osobních údajů. Uchovávání fotografií není samo o sobě považováno za zpracování citlivých osobních údajů o rasovém či etnickém původu, pokud nedochází k dalšímu zpracování, například třídění podle biometrických charakteristik vypovídajících o rasovém nebo etnickém původu, připojování slovně vyjádřených údajů o rasovém nebo etnickém původu k jednotlivým fotografiím a podobně.[81]

V praxi jsou fotografie nejčastěji uchovávány zaměstnavatelem za účelem vydání služebního průkazu, tak z hlediska Zákonu o ochraně osobních údajů se

[79] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 168
[80] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 169
[81] BARTÍK Václav; JANEČKOVÁ Eva. – Fotografie v osobním spisu zaměstnance z hlediska zoou In práce a mzda 9/2012

jedná o zpracování dle §5 odstavec 2 písmeno a), tedy „*zpracování nezbytné pro dodržení právní povinnosti správce, tedy zaměstnavatele*“.[82] V tomto případě není vyžadován souhlas zaměstnance, naopak pokud se jedná o pracovní místo vyžadující služební průkaz, má zaměstnanec povinnost zaměstnavateli fotografii poskytnout, ten ji ale může použít jen pro stanovený účel.[83] Pokud je jiný důvod, měl by mít zaměstnavatel souhlas zaměstnance s použitím jeho profilové fotografie, pokud se nejedná o výjimku jakou je ustanovení §5 odstavec 2 písmeno e) Zákona na ochranu osobních údajů, *tedy je-li to nezbytné k ochraně práv a právem chráněných zájmů správce*.[84]Pokud se bude jednat o jiné důvody, než jsou uvedeny v ustanovení §5 odstavci 2, je vždy vyžadován souhlas zaměstnance s použitím jeho fotografie.

Pokud se jedná o jinou než průkazovou fotografii, například fotografie ze společenských akcí zaměstnavatele, teambuildingů, konferencí a podobně, jsou tyto fotografie označeny pouze názvem akce, a ne jinými údaji, ze kterých by bylo možné identifikovat subjekty údajů na ní zachycené, nebude se jednat o zpracování osobních údajů ve smyslu §4 písmena e) Zákona na ochranu osobních údajů a při jejich zpracování tak nedochází k zásahu do práva na ochranu osobních údajů.[85]

Zpracování osobních údajů po ukončení pracovního poměru

Skončením pracovního poměru se právní základ velmi omezuje, to neznamená ale, že bývalý zaměstnavatel ztrácí právo zpracovávat některé osobní údaje bývalého zaměstnance. K takovému zpracování, ale musí bývalý zaměstnavatel mít právní základ, může se jednat o účel archivnictví, penzijního pojištění a podobně. Dalším důvodem k uchovávání osobních údajů bývalého zaměstnance je soudní spor, v tomto případě bývalý zaměstnavatel uchovává osobní údaje zaměstnance až do skončení sporu.[86]

---

[82] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 odstavec 2 písm. a)

[83] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013. s. 169

[84] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 odstavec 2 písm. e)

[85] BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 2. vydání, Praha: Linde Praha 2013. s. 153 a následující

[86] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

I po skončení pracovního poměru, má bývalý zaměstnanec nárok na přístup k informacím, které o něm bývalý zaměstnavatel shromažďuje na základě právního titulu. Jedná se totiž stále o správce jeho osobních údajů. Bývalý zaměstnanec si tak může zkontrolovat, jestli jeho osobní údaje jsou využívány jen k účelu, který umožňuje zákon. Platí zde zásada proporcionality, což znamená, že osobní data, která shromažďuje bývalý zaměstnavatel, musejí sloužit jen pro naplnění daného účelu, a to jen na nezbytnou dobu. V případech kdy zákon nestanoví či neumožní zpracovávat osobní informace, musí je bývalý zaměstnavatel neprodleně zlikvidovat. [87]

„Pokud je podezření, že bývalý zaměstnavatel nesplňuje povinnosti se zpracováním osobních údajů, má bývalý zaměstnanec právo podat stížnost příslušnému orgánu ochrany osobních údajů. Je to z důvodu toho, že byť je zaměstnavatel bývalý, je stále správcem osobních dat bývalého zaměstnance.“[88]

„Předání osobních údajů od bývalého zaměstnavatele k současnému je možné pouze tehdy, pokud bývalý zaměstnavatel k tomu má právní titul. Tím může být souhlas bývalého zaměstnance, anebo povinnost, kterou mu stanovuje zákon. Bývalý ani současný zaměstnavatel nemohou zveřejnit osobní údaje, které se netýkají pracovněprávního vztahu.“[89]

[87] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

[88] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

[89] Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

4) Pojmy podle GDPR

Pseudonymizace

„Pseudonymizací se rozumí zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“[90]

Osobní údaje dle obecného nařízení EU 2016/679 - GDPR

„Definice osobních údajů podle obecného nařízení GDPR je v článku 4 odstavec 1 Nařízení EU 2016/679 a zní: „osobními údaji" 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;“[91]

Osobní údaje se dělí na:

- *Obecné osobní údaje – jméno, příjmení, datum narození*
- *Organizační osobní údaje – telefonní číslo, e-mail, IP adresa*
- *citlivé osobní údaje – zvláštní kategorie osobních údajů jako jsou politické názory, zdravotní stav, genetické a biometrické údaje*[92]

Speciální zacházení vyžadují zvláštní kategorie osobních údajů, uvedené v článku 9 Nařízení GDPR a v následující kapitole této práce.

Nařízení GDPR ve svém článku 10 upravuje zpracování osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů: „*Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících*

[90] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(5)
[91] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(1)
[92] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 49

bezpečnostních opatření na základě článku 6 odst. 1 se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci.“[93]

Osobní údaje je možné dle Nařízení GDPR zpracovávat na základě právních titulů, které v článku 6 odstavec 1 stanovuje šesti různými právními tituly, které umožňují zpracování osobních údajů: „Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

> *a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*
>
> *b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
>
> *c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
>
> *d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*
>
> *e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
>
> *f) 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. První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.*[94]

[93] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 10
[94] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 6(1)

Zvláštní kategorie osobních údajů

Článek 9 Nařízení GDPR odstavec 1 taxativně určuje, o které osobní údaje se jedná. Jsou to: *„rasový a etnický původ, politické názory, náboženské vyznání, filosofické přesvědčení, členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby, zdravotní stav, sexuální orientace a sexuální život.“ A zároveň zakazuje zpracování těchto informací*.[95]

Zároveň ve svém druhém odstavci stanovuje výjimky, za kterých je možné zpracovávat osobní údaje zvláštní kategorie: „

> *a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;*
>
> *b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;*
>
> *c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;*
>
> *d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;*

[95] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9(1)

e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;

f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků, nebo pokud soudy jednají v rámci svých soudních pravomocí;

g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;

h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;

i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů. "[96]

[96] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9(2)

„Členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů a údajů o zdravotním stavu.[97]

Článek 4 odstavce 13-15 Nařízení GDPR

Genetické údaje Nařízení GDPR definuje jako: *„…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*;“[98]

Biometrické údaje Nařízení GDPR definuje jako: *„…osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;“*[99]

Údaje o zdravotním stavu Nařízení GDPR definuje jako:*“… osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.“*[100]

Dynamický a biometrický podpis

Dynamický elektronický podpis neboli digitální či elektronický podpis, umožňuje rozpoznání biometrických prvků. Na speciálním zařízení se snímá fyzický podpis, který je převáděn do elektronické podoby. Dochází k zachycení grafické podoby, tlaku, sklonu písma a dalších vlastností podpisu. Grafické znázornění a biometrické údaje podpisu jsou tak zaznamenávány a uchovávány společně. Následně je podpis převeden do elektronické podoby a připojen k dokumentu.

Samotné podepsání dokumentu ještě není zpracováním osobního údaje, pokud se jedná o podpis na papír, avšak pokud se jedná o podpis na speciální zařízení snímající fyzický podpis, jak bylo naznačeno výše, už se o zpracování

[97] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9(4)
[98] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(13)
[99] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(14)
[100] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(15)

osobních údajů jedná, protože zařízení snímá jak grafickou podobu, tak i dynamické vlastnosti písma.

Samotné pořízení a uchování podpisu bez jeho dalšího využití není zpracováním osobních údajů. Ke zpracování zvláštní kategorie osobních údajů dochází až tehdy, když je podpis podroben písmoznalecké analýze za účelem ověření pravosti v případě sporu a podobně. O zpracování zvláštní kategorie osobních údajů půjde, pokud tyto údaje jsou správcem aktivně využívány.

Zpracování osobního údaje v podobě podpisu je možné na základě právního titulu uzavření a splnění smlouvy. Co se týče dynamického biometrického podpisu, ten lze zpracovávat jen s výslovným souhlasem dotčené osoby. Pokud subjekt údajů odmítne použít dynamický biometrický podpis, musí mu správce údajů dát možnost podepsat se klasickým způsobem na papír.[101]

Balanční testy

V balančním testu správce údajů posuzuje, jestli nad jeho oprávněným zájmem nepřevyšují práva a svobody subjektu údajů. Správce musí posoudit přiměřenost svého oprávněného zájmu vzhledem k právům subjektu údajů, a to právě pomocí balančního testu, který obsahuje následující markanty: význam oprávněného zájmu správce, hrozící riziko pro subjekt osobních údajů, jehož osobní údaje jsou vyhodnocovány, očekávání subjektu osobních údajů při zpracování, míru bezpečnostních opatření a samozřejmě vyhodnocení.[102]

Pokud výsledek vyjde ve prospěch správce, může osobní údaje subjektu zpracovávat na základě právního důvodu „oprávněný zájem správce“. Informační povinnost vůči subjektu osobních údajů mu ale tímto nezaniká a správce osobních údajů musí subjektu uvést, v čem přesně spočívá jeho oprávněný zájem.[103]

Stanovisko Úřadu pro ochranu osobních údajů zní takto: *„Správce je povinen provést balanční test, neboli test proporcionality, pro každé zpracování osobních údajů, které hodlá vykonávat na základě právního důvodu oprávněného zájmu.*

[101] STAŇKOVÁ Lucie. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 58

[102] TESAŘ Jan. Balanční test- GDPR. [online]. 2019 [cit. 22. 3. 2019]. Dostupné z: http://www.guard7.cz/gdpr/balancni-test-gdpr

[103] TESAŘ Jan. Balanční test- GDPR. [online]. 2019 [cit. 22. 3. 2019]. Dostupné z: http://www.guard7.cz/gdpr/balancni-test-gdpr

Balanční test by měl být vypracován ve vztahu k účelu zpracování, přičemž pro obdobné účely postačuje vypracování jednoho balančního testu. Právě v důsledku takového testu je pak správce schopen vyhodnotit, zda před jeho oprávněnými zájmy nemají přednost zájmy nebo práva a svobody subjektu údajů, a lze tak tento právní důvod pro zpracování osobních údajů využít.“[104]

Kodexy chování

Jedná se o důležitý prvek posouzení rizik, rozlišujeme mimo jiné vnitropodnikové kodexy chování, případně kodexy podnikatelských sdružení pro oblast ochrany údajů. Kodexy chování přispívají k bezpečnému chování při správě a zpracování osobních údajů a slouží jako určité vodítko k uplatňování správné praxe při správě a zpracování osobních údajů.

Podle Jiřího Navrátila by měly obsahovat:

- *zákonné a transparentní zpracování osobních údajů*
- *respektování oprávněných zájmů správců osobních údajů v konkrétních situacích*
- *obecná pravidla pro bezpečné a především zákonné shromažďování osobních údajů*
- *využívání pseudonymizace*
- *optimální míru informování veřejnosti a subjektu údajů a ochraně osobních údajů v podniku*
- *zajištění výkonu práv subjektů údajů*
- *zajištění řádného a především srozumitelného poskytování informací dětem v souvislosti se shromažďováním a zpracováním jejich osobních údajů, včetně způsobu získávání souhlasu jejich zákonných zástupců (rodičů)*

[104] Úřad pro ochranu osobních údajů. Právní důvody zpracování. [online]. 2018 [cit. 25. 3. 2019]. Dostupné z: https://www.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=3938

- *podmínky předávání osobních údajů do třetích zemí nebo mezinárodním organizacím*
- *podmínky a principy spravedlivého mimosoudního vyrovnání s osobami poškozenými chybami při správě a zpracování osobních údajů a jiné postupy pro řešení sporů mezi správci a fyzickými osobami jako subjekty údajů v souvislosti se zpracováním.*[105]

Tyto kodexy se registrují u Úřadu pro ochranu osobních údajů, který posoudí, zda jsou v souladu s Nařízením. Pokud Úřad uzná, že tento návrh, popřípadě jeho úprava či rozšíření schváleného kodexu splňuje záruky pro ochranu osobních údajů, kodex schválí. Může se stát, že jeden kodex se bude vztahovat na území ve více členských státech Evropské unie. Jiří Navrátil ve své publikaci „GDPR pro praxi“ očekává v budoucnu vznik „centrální knihovny kodexů Evropské unie“, z důvodu co možná nejlepší informovanosti veřejnosti o těchto kodexech.[106]

Kontrolu nad těmito kodexy a jejich úřední monitorování provádějí subjekty jmenované Úřadem pro ochranu osobních údajů, které prokáží svoji odbornou znalost v oblasti, pro kterou je kodex určen, znalost v ochraně osobních údajů a se zkušenostmi s prováděním auditů.[107]

4.1. Kontrola ve firmě

Veškerá opatření zavedená pro soulad s Nařízením GDPR musí být pravidelně kontrolována a aktualizována. Proto je potřeba vypracovat plán kontroly souladu s Nařízením GDPR. Kontrola patří mezi jedno z organizačních opatření, které pomáhají zajistit správné plnění povinností určených Nařízením GDPR.

[105] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 106
[106] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk s. 106-107
[107] Úřad pro ochranu osobních údajů. Kodexy chování [online]. 2018 [cit. 25. 3. 2019]. Dostupné z: https://www.uoou.cz/kodexy-chovani/d-29493/p1=4818

Objevují se nová rizika, hodnota osobních údajů se pro firmu může různě měnit, mohou být použity nové informační systémy. Veškeré změny nebo nové postupy zpracování a ochrany osobních údajů musí být vždy v souladu s Nařízením GDPR.

Z každé kontroly musí být proveden záznam, který bude uchován pro případ kontroly ze strany dozorového úřadu, což je v České republice Úřad pro ochranu osobních údajů.

„V rámci kontroly souladu s Nařízením GDPR by se mělo:

- *posoudit a zhodnotit nakládání s osobními údaji, především z hlediska jejich nezbytnosti a zabezpečení,*
- *posoudit a zhodnotit rizika pro práci s osobními údaji a pravděpodobnost jejich výskytu,*
- *zvážit, zda je skutečně nutné získávat souhlas se zpracováním osobních údajů od subjektu údajů, nebo zda je možné využít jiný právní titul pro zpracování,*
- *přijmout další vhodná opatření jak technologická, tak organizační pro ochranu osobních údajů, pokud je to nutné*
- *posoudit a zhodnotit plnění povinností ve vztahu k subjektům údajů*
- *posoudit a zhodnotit plnění povinností ve vztahu k dozorovému* úřadu“[108]

Pro kontrolu práce s osobními údaji by měl mít ve firmě správce osobních údajů, případně jejich zpracovatel, který má přehled o tom, jak zaměstnanci s osobními údaji pracují. Na pomoc jim zpravidla slouží informační systém, které dokáže sám zaznamenávat kdo, kdy a jak s daty pracuje a zpracovávají takzvané logy, tedy přihlášení a přístupy do jednotlivých částí informačního systémů. Pro dokola od souladu s Nařízením GDPR je proto vhodné tyto informace ukládat.

Pokud je v jedné firmě více správců nebo zpracovatelů, musí původní správce zajistit, aby zpracování od jiného správce, případně zpracovatele, bylo také v souladu s Nařízením GDPR. Kontrolu s Nařízením GDPR je vhodné vypracovat ve spolupráci s pověřencem pro ochranu osobních údajů, pokud ve

[108] STAŇKOVÁ Lucie. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 59

firmě byl jmenován, popřípadě s jinou osobou, která je za zpracování dat zodpovědná.[109]

„*Kontrola by měla být provedena vždy, pokud dojde k:*

- *zavedení nových právních předpisů*
- *zavedení nových technologií*
- *zavedení nových postupů a procesů*
- *zavedení nových opatření*
- *a podobně*“[110]

K tomu by měla být prováděna pravidelná kontrola souladu s Nařízením GDPR, která by měla být minimálně jednou za 2 roky. Pravidelné hodnocení a přezkoumávání musí probíhat zejména u zavedených kodexů chování (viz pojmy Nařízení).

„*Správce údajů zavádí technická a organizační opatření pro ochranu osobních údajů podle svého nejlepšího vědomí a svědomí. Protože stále dochází k vývoji nástrojů a postupů pro zpracování dat, musí být prováděno pravidelné testování, posuzován a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*“[111]

Jednou ze zásad Nařízení je i zásada omezení uložení. Z toho plyne, že doba uložení by neměla být delší, než je nezbytné pro účely zpracování. Aby osobní údaje nebyly uchovávány déle, než je nezbytné, měl by správce stanovit lhůty pro výmaz nebo pravidelnou kontrolu zpracovaných osobních údajů.

„*V případě předávání osobních údajů do třetích zemí nebo předávání mezinárodním organizacím je nezbytné sledovat posouzení Komise o odpovídající ochraně. Schválená rozhodnutí musí být Komisí přezkoumávána minimálně každé 4 roky.*“[112]

[109] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 59

[110] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 60
[111] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 60
[112] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 60

Zkontrolovány by měly být i další vnitropodnikové směrnice a předpisy, aby neobsahovaly pokyny nebo procesy, které už nejsou v souladu s Nařízením GDPR.

Webové stránky mohou být nastaveny tak, že shromažďují a zpracovávají osobní údaje návštěvníků, a tato skutečnost nemusí být uživatelům hned zřejmá. Proto je zapotřebí zkontrolovat i webové stránky.

Kontrola dozorového úřadu

Kontrola ze strany dozorového úřadu probíhá prostudováním předložených dokumentů, otázek a pohovorů. Dozorující úřad také může navštívit firmu a udělat vizuální prohlídku a vyzkoušet vybrané nástroje pro zpracování osobních údajů.

Ve firmě by tak měla existovat dokumentace, která bude prokazovat vše potřebné pro dokázání souladu s Nařízením GDPR. V této složce by měly být obsaženy především tyto dokumenty:

- *„Výsledky analýzy současného stavu (zpracování osobních údajů před zavedením požadavků určených Nařízením GDPR; to se nevztahuje na firmy, které začaly na trhu působit až po 25. květnu 2018, jelikož ty musí plnit Nařízení GDPR od svého vzniku,*
- *výsledky analýzy rizik,*
- *směrnice o ochraně osobních údajů,*
- *archivační a skartační řád,*
- *informace o zpracování osobních údajů pro subjekt údajů a další veřejnost,*
- *podklady pro plnění práv subjektů údajů,*
- *záznamy o činnostech zpracování osobních údajů (pokud má správce povinnost je vést),*
- *podklady pro oznamování a ohlašování případů porušení zabezpečení,*
- *souhlasy se zpracováním osobních údajů (pokud správce tento právní titul pro zpracování osobních údajů využívá),*

- *balanční testy (pokud správce používá jako právní titul pro zpracování osobních údajů oprávněný zájem),*
- *zpracovatelské smlouvy (pokud správce nevyužívá vlastního Zpracovatele osobních údajů),*
- *podklady pro Pověřence pro ochranu osobních údajů (pokud ho musí jmenovat) nebo alespoň pro osobu odpovědnou za ochranu osobních údajů ve firmě,*
- *podklady pro posouzení vlivu na ochranu osobních údajů (pokud ho správce musí vypracovat),*
- *záznam o proškolení zaměstnanců o problematice Nařízení GDPR,*
- *plán kontroly souladu s Nařízením GDPR,*
- *pravidla pro předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (pokud k takovému předávání dochází),*
- *závazná podniková pravidla (pokud je zpracování osobních údajů prováděno v rámci skupiny podniků, které si předávají osobní údaje přes hranice).“*[113]

V České republice je dozorovým úřadem Úřad pro ochranu osobních údajů, který kontroluje na základě vlastního plánu kontrol nebo na podnět fyzické či právnické osoby.

Rozsah, množství a postup kontroly dozorový úřad oznamuje předem a kontroly jsou prováděny v souladu s Nařízením GDPR a zákonem č. 255/2012 Sb., o kontrole.

Dalším, kdo je zmocněn ke kontrole, je Nejvyšší kontrolní úřad, a to podle článku 97 Ústavy a Zákona č.166/1993 Sb., o Nejvyšším kontrolním úřadu. Pokud by kontrolu zpracování údajů prováděl NKÚ, právním titulem bude plnění úkolu ve veřejném zájmu, popřípadě při výkonu veřejné moci.[114]

Při kontrole Úřadu pro ochranu osobních údajů nejčastěji dochází ke zkoumání:

[113] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 61
[114] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 62

- *„rozsahu a formy zpracování osobních údajů, především zvláštní kategorie osobních údajů, jejich anonymizování a předávání,*
- *logování jednotlivých operací s osobními údaji,*
- *evidence a oprávněnosti přístupů k osobním údajům,*
- *existence poučení pracovníků a výkon jejich práce v souladu s Nařízením GDPR,*
- *existence souhlasů se zpracováním osobních údajů a jejich předáváním třetím stranám,*
- *náležitostí zpracovatelských smluv,*
- *a podobně"*[115]

Faktory pro posouzení nedodržení Nařízení GDPR

- *„Dosavadní činnost správce údajů související se stížnostmi podanými dozorovému úřadu a reakcemi správce na tyto stížnosti,*
- *provedená hlášení o bezpečnostních incidentech a o nápravných opatřeních realizovaných správcem,*
- *komunikace se správcem, především jeho reakce na upozornění ohledně nedostatků při zpracování osobních údajů,*
- *informace získané z novinových zpráv ve veřejném prostoru, které zdůrazňují problémy a nedostatky správce při zpracování osobních údajů,*
- *informace od dalších dozorových a regulačních orgánů,*
- *informace zveřejněné správcem údajů, které se vztahují k problematice ochrany a zpracování osobních údajů,*
- *výsledky interních a externích auditů prováděných u správců a zapojených zpracovatelů,*
- *závěry dosavadních kontrol*
- *informace o zavádění nových systémů a postupů,*
- *rozsah a povaha zpracování osobních údajů,*
- *existence kodexů chování, osvědčení, certifikátů, známek nebo pečetí,*
- *dopady nesouhlasu s Nařízením GDPR na subjekty údajů,*

[115] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s.62

- *další relevantní informace – například závěry vyhotoveného posouzení vlivu na ochranu osobních údajů.“*[116]

Pokud dojde ke zjištění nedostatků, dozorující úřad bude požadovat nápravu podle závažnosti porušení daného článku Nařízení GDPR. Na výběr má od varování, přes napomenutí a pozastavení zpracování údajů, až možnost uložit pokutu.[117]

4.2. Sankce

„Sankční část bývá zpravidla součástí každé právní normy a ta má jak preventivní, tak donucující účinek na adresáty. Vlastně pod hrozbou sankce nutí adresáty chovat se podle normou stanovených pravidel. Toto Nařízení má svou sankční část uvedenou v článku 83, kde stanovuje podmínky pro uložení pokut a jejich možnou výši.“[118]

Článek 83: *„Obecné podmínky pro ukládání správních pokut:*

(1) Každý dozorový úřad zajistí, aby ukládání správních pokut v souladu s tímto článkem ohledně porušení tohoto nařízení podle odstavců 4, 5 a 6 bylo v každém jednotlivém případě účinné, přiměřené a odrazující.

(2) Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j). Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

[116] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 62
[117] STAŇKOVÁ LUCIE. *GDPRsnadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 63
[118] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018 s. 185

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

(3) Pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací zpracování poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení.

(4) Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) povinnosti správce a zpracovatele podle článků 8, 11, 25 až 39, 42 a 43;

b) povinnosti subjektu pro vydávání osvědčení podle článků 42 a 43;

c) povinnosti subjektu pro vydávání osvědčení podle čl. 41 odst. 4.

(5) Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) základní zásady pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9;

b) práva subjektů údajů podle článků 12 až 22;

c) předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle článků 44 až 49;

d) jakékoli povinnosti vyplývající z právních předpisů členského státu přijatých na základě kapitoly IX;

e) nesplnění příkazu nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1.

(6) Za nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 lze v souladu s odstavcem 2 tohoto článku uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší.

(7) Aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

(8) Na výkon pravomocí dozorovým úřadem podle tohoto článku se vztahují vhodné procesní záruky v souladu s právem Unie a členského státu, včetně účinné soudní ochrany a spravedlivého procesu.

(9) Neumožňuje-li právo členského státu uložení správních pokut, může se použít tento článek tak, aby podnět k uložení pokuty dal příslušný dozorový úřad a aby pokuta byla uložena příslušnými vnitrostátními soudy, a současně je třeba zajistit, aby tyto prostředky právní ochrany byly účinné a aby jejich účinek byl rovnocenný se správními pokutami, jež ukládají dozorové úřady. Uložené pokuty musí být v každém případě účinné, přiměřené a odrazující. Tyto členské státy oznámí Komisi do 25. května 2018 příslušná ustanovení svých právních předpisů, která přijmou podle tohoto odstavce, a bez prodlení jakékoliv následné novely nebo změny týkající se těchto ustanovení.“[119]

[119] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 83

Při rozhodování o tom, zda pokutu uložit, a při rozhodování o její výši musí dozorový úřad zohlednit následující okolnosti:

- *„Povahu, závažnost a délku trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byl způsobena,*
- *zda k porušení došlo úmyslně nebo z nedbalosti,*
- *kroky podniknuté ke zmírnění škod způsobených subjektům údajů,*
- *míru odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedených dle článků 25 a 32 Nařízení,*
- *veškerá relevantní předchozí porušení správcem či zpracovatelem,*
- *míru spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků,*
- *kategorie osobních údajů dotčené daným porušením,*
- *způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámili, a pokud ano, v jaké míře,*
- *v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízená opatření uvedená v článku 58 odstavec 2 Nařízení GDPR, splnění těchto opatření,*
- *dodržování schválených kodexů chování nebo schváleného mechanismu pro vydání osvědčení,*
- *jakoukoliv jinou přitěžující nebo polehčující okolnost, jako je finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývajících z porušení.“*[120]

Nařízení GDPR dává poměrně velkou variabilitu při ukládání pokut, včetně neuložení, kdy lze uložit buď samostatně, nebo s pokutou některá z nápravných opatření podle článku 58 odstavec 2 písmena a) – h) a j) Nařízení

[120] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018 s. 186

GDPR. Pokud už bude udílena, bude se přihlížet k výše zmiňovaným okolnostem, které ovlivní její výši.[121]

Článek 58 odstavec 2 Nařízení:

a) *upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;*

b) *udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;*

c) *nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;*

d) *nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;*

e) *nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;*

f) *uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;*

g) *nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a článku 19;*

h) *odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;*

i) *uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;*

j) *nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.“*[122]

Pokud se bude jednat o bagatelní případ s minimální společenskou škodlivostí, s velkou pravděpodobností nebude pokuta vůbec udělena, postačí jiné z nápravných opatření, popřípadě jen informovat správce o jeho povinnostech, a

[121] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018.s.187
[122] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 58(2)

bude se čekat, že správce sám na základě informací uvedených v dopise uvede vše do souladu s Nařízením GDPR.[123]

„*Tento postup je v souladu se Zákonem o odpovědnosti za přestupky a řízení o nich, podle kterého se pokuty procesně projednávají, a který upravuje takzvanou materiálně-formální definici přestupku, kdy ke spáchání musí, kromě skutkové podstaty, být přítomna i materiální stránka, což znamená společenská škodlivost protiprávního činu.*“[124]

Promlčecí doba je stanovena v §30 Zákona o odpovědnosti za přestupky a řízení o nich. Pro přestupky spočívající v Nařízení GDPR platí tříletá promlčecí lhůta, protože se jedná o čin, za který Zákon stanoví sazbu pokuty, jejíž horní hranice je alespoň 100 000 Kč.[125]

První pokuty plynoucí z Nařízení GDPR

Jednou z prvních firem, která byla sankciována, byl americký internetový velikán Google LLC. 21. ledna letošního roku mu dozorčí úřad ve Francii udělil pokutu čítající 50 000 000EUR. Řízení bylo zahájeno na podnět cirka 10 000 podpisů.

„*Vyčítány byly nedostatky v transparentnosti a informování. Úřad konstatoval, že nebyla dostatečně splněná informační povinnost, protože informace poskytované subjektům údajů nebyly lehce přípustné. Struktura informací o zpracování osobních údajů nebyla v souladu s Nařízením GDPR, jelikož podstatné informace, jako účel zpracování, doba uložení či kategorie osobních údajů zpracovávaných za účelem personalizace reklam byly nekompaktně roztroušeny v několika samostatných dokumentech. Relevantní informace byly dostupné ze strany subjektu údajů až po šestém prokliku.* “[126]

Dále úřad konstatoval, že některé informace byly nedostatečně vysvětleny, a díky tomu uživatelé neměli šanci rozumět rozsahu zpracovatelských operací.

---

[123] ŽŮREK Jiří. Kontrola automaticky neznamená udělení pokuty. [online]. 2018 [cit. 26. 3. 2019]. Dostupné z: https://www.uoou.cz/kontrola-automaticky-neznamena-udeleni-pokuty/d-31861

[124] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 188

[125] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 188

[126] MAĎAROVÁ Helga. První pokuty za porušení GDPR jsou na světě. [online]. 27. 2. 2019 [cit. 26. 3. 2019]. Dostupné z: https://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-*GDPR*-jsou-na-svete-108915.html

Současně nebyl uveden souhlas jako právní základ pro personalizaci reklam a doby uložení pro některé kategorie údajů nebyly uvedeny vůbec.

Další věc, kterou úřad internetovému gigantu vytýkal, byl neplatný souhlas pro personalizaci reklam. Google zpracovává osobní údaje za účelem personalizace reklam, a to na základě souhlasu. Jenže úřad konstatoval, že souhlasy subjektů údajů nebyly platně poskytnuty právě kvůli nedostatečnému informování subjektů údajů. Předmětné informace byly opět ve více dokumentech a průměrný uživatel neměl šanci porozumět tomu, že za účelem reklamy se zpracovávají jeho údaje zkombinované z různých služeb, jimiž jsou Google, Youtube a podobně.

„*Souhlas měl být dán neplatně také proto, že byl udělen prostřednictvím dopředu označeného nástroje, a současně proto, že souhlas mohl být dán pouze souhrnně pro všechny v něm uvedené zpracovatelské operace bez možnosti vynětí některých operací. Postup tak nesplňoval požadavek, aby byl souhlas udělený pro každý účel zpracování samostatně. Na základě výše uvedeného konstatování ze strany Úřadu je možné vyvodit kritéria pro transparentnost, efektivní informování a udělování souhlasu. Zajímavostí však je, že řízení bylo vedeno vůči společnosti Google LLC se sídlem v USA a ne proti její evropské centrále sídlící v Irsku (v tomto případě by totiž byl pro řízení příslušný irský, a ne francouzský regulátor). Důvodem tohoto postupu bylo zjištění, že v souvislosti s aktivitami, které byly předmětem kontroly, neměla irská společnost Google žádnou rozhodovací pravomoc a za správce se tedy považovala výlučně americká mateřská společnost. V této souvislosti bude velmi zajímavé sledovat, jak se k vykonatelnosti sankce uložené evropským orgánem vůči subjektu sídlícímu mimo EU postaví dotčené subjekty. S ohledem na silné postavení společnosti Google LLC na evropském trhu bude do určité míry precedentní, jak bude v praxi fungovat ambiciózní ustanovení GDPR o jeho působnosti i mimo území EU.*“[127]

[127] MAĎAROVÁ Helga. První pokuty za porušení GDPR jsou na světě. [online]. 27. 2. 2019 [cit. 26. 3. 2019]. Dostupné z: https://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-*GDPR*-jsou-na-svete-108915.html

5) Právní tituly podle GDPR

Nařízení GDPR v článku 6 odstavci 1 stanovuje 6 různých titulů (viz výše)[128]

„Aby zpracování osobních údajů bylo zákonné, stačí, aby bylo takové zpracování prováděno na základě jednoho právního titulu. Naopak, pro stejný účel zpracování by se neměly právní tituly kumulovat.“[129]

Zákonné plnění – právní povinnost:

Základ pro zpracování osobních údajů musí být stanoven právem Evropské unie nebo členského státu, který se na správce vztahuje. Jedná se o velkou část zpracování osobních údajů zaměstnanců. Dané zákony zpracování jsou například Zákon o archivnictví, Zákon o dani z příjmu a podobně.[130]

[128] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 6(1)
[129] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 28
[130] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 29

6) Práva subjektu údajů

Nařízení GDPR přiznává subjektu údajů (zaměstnanci) 12 práv, mezi které patří:

1) *právo na přístup k informacím,*
2) *právo opravu osobních údajů,*
3) *právo být zapomenut,*
4) *právo na omezení zpracování osobních údajů,*
5) *právo na přenositelnost osobních údajů,*
6) *právo vznést námitku,*
7) *právo nebýt předmětem automatizovaného rozhodování,*[131]
8) *právo podat stížnost u dozorového úřadu,*
9) *právo na účinnou soudní ochranu – vůči dozorovanému úřadu a vůči správci nebo zpracovateli,*
10) *právo na zastoupení subjektu údajů,*[132]
11) *právo na náhradu újmy a odpovědnost,*[133]
12) *právo odvolat souhlas.*[134]

„Informace o přijatých opatřeních ohledně výkonu práv subjektů údajů musí být sděleny bez zbytečného odkladu a v každém případě nejpozději do 1 měsíce o obdržení žádosti o výkon práv. Tato lhůta se může posunout v případě nutnosti a s ohledem na složitost případu, popřípadě počtu žádostí o další 2 měsíce. Správce však musí informovat subjekt údajů o takovémto prodloužení, a to do 1 měsíce od obdržení žádosti spolu s důvodem, proč k odkladu dochází.“[135]

Správci, v případech důvodné pochybnosti totožnosti subjektů, musí provést takzvaný postup ověřování, kterým se spolehlivě prokáže totožnost subjektu údajů, který uplatňuje práva přiznaná Nařízením GDPR. Příkladem

[131] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 15 -23
[132] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 77 – 80
[133] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 82
[134] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 7(3)
[135] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 31

postupu ověřování může být žádost o upřesňující údaje, popřípadě potvrzovací zpráva, SMS nebo email.[136]

Poskytování činností souvisejících s právy subjektu údajů se provádějí bezplatně. Pokud jsou žádosti subjektu údajů neopodstatněné, opakující se nebo nepřiměřené, může správce uložit přiměřený poplatek, který bere v potaz administrativní náklady spojené s poskytnutím požadovaných údajů. V závažných případech může správce dokonce odmítnout vyhovět žádosti subjektu údajů, nicméně toto je skutečně krajní řešení a mělo by být využíváno co možná nejméně.[137]

„*Pokud správce nepřijme opatření, o které subjekt údajů zažádal, musí se tak bezodkladně vyjádřit, nejpozději však do 1 měsíce od přijetí žádosti. Musí udat důvody, proč žádost nepřijal a informovat o možnosti podat stížnost dozorovému úřadu a žádat soudní ochranu. Správci jsou vázáni povinností odpovídat ve stanovených lhůtách, a to i v případě, že odmítají. Zkrátka, správci se musejí k žádosti subjektu údajů vždy vyjádřit.“*[138]

„Při nedodržení výkonu práv subjektů údajů, hrozí správci sankce, které mají maximální hodnotu až 20 000 000 EUR, popřípadě 4 % celkového ročního obratu firmy celosvětově, záleží, která z hodnot je vyšší, a ta bude aplikována.“[139]

Právo na přístup k osobním údajům

Subjekt údajů má právo získat od správce potvrzení, zda údaje, které se ho týkají, jsou nebo nejsou zpracovány, a pokud tomu tak je, má právo získat přístup k těmto osobním údajům a k informacím ohledně účelu zpracování, ohledně kategorie dotčených osobních údajů, ohledně příjemců, kterým osobní údaje budou zpřístupněny, zejména pak ohledně příjemců ve třetích zemích, popřípadě mezinárodních organizacích. Dále mají subjekty údajů právo vědět, jaká je plánovaná doba, po kterou budou osobní údaje uloženy, nebo pokud není možné ji určit, tak jaká jsou kritéria použitá ke stanovení této doby. [140]

[136] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 31
[137] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 31
[138] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 31
[139] STAŇKOVÁ LUCIE. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018 s. 31
[140]ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 136

Právo na opravu

Přímá definice práva na opravu je uvedena v článku 16 Nařízení GDPR a zní*: „Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.“*[141]

Právo na výmaz = právo být zapomenut

Jedno ze základních práv subjektu údajů je, aby správce bezodkladně vymazal osobní údaje, které se právě toho subjektu týkají, pokud k tomu byl dán jeden z důvodů uvedených v článku 17 odstavec 1 písmena a) až f) a v odstavci 2, kde je řečeno, že:

„a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2;

e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;

f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1.“[142]

„*V případě, že správce osobní údaje zveřejnil, je povinen je vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené*

[141] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 16
[142] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 17 (1) písmena a)-f)

kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie nebo replikace.“[143]

Právo na výmaz údajů nemůže subjekt údajů uplatnit v případech, které jsou uvedeny ve 3. odstavci článku 17 Nařízení GDPR: „

a) pro výkon práva na svobodu projevu a informace

b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;

c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3;

d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;

e) pro určení, výkon nebo obhajobu právních nároků.“[144]

Právo na omezení zpracování

Právo subjektu údajů na omezení zpracování je definováno v článku 4 odstavec 3 Nařízení GDPR, které omezením zpracování rozumí: *„…označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu“*.[145]

(*1) Subjekt údajů má právo na to, aby správce omezil zpracování, v kterémkoli z těchto případů:*

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;

[143] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 17(2)
[144] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 17(3) písm. a) - e)
[145] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(3)

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

(2) Pokud bylo zpracování omezeno podle odstavce 1, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.

(3) Subjekt údajů, který dosáhl omezení zpracování podle odstavce 1, je správcem předem upozorněn na to, že bude omezení zpracování zrušeno.“[146]

Právo na přenositelnost údajů

Právo na přenositelnosti údajů je definováno v článku 20 Nařízení GDPR:„

(1) Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému

[146] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 18(1) – 18(3)

byly osobní údaje poskytnuty, bránil, a to v případě, že:

a) zpracování je založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1 písm. b); a

b) zpracování se provádí automatizovaně.

(2) Při výkonu svého práva na přenositelnost údajů podle odstavce 1 má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

(3) Výkonem práva uvedeného v odstavci 1 tohoto článku není dotčen článek 17. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

(4) Právem uvedeným v odstavci 1 nesmí být nepříznivě dotčena práva a svobody jiných osob.“[147]

Podle Žůrka je ideou tohoto práva umožnění uživatelů přechod mezi poskytovateli služeb na sektorové úrovni a zvětšení konkurenceschopnosti. I když toto právo připomíná právo na přístup k osobním údajům, není tak univerzální. Jak je vidět v předchozím odstavci, aplikace práva na přenositelnost je omezena podmínkami, které musejí být kumulativně splněny.[148]

Právo vznést námitku

Právo vznést námitku je definováno v článku 21 Nařízení GDPR:

(1) Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, na základě čl. 6 odst. 1 písm. e) nebo f), včetně profilování založeného na těchto ustanoveních. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné

[147] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 20
[148] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 143

oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

(2) Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu.

(3) Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou, již osobní údaje pro tyto účely zpracovávány.

(4) Subjekt údajů je na právo uvedené v odstavcích 1 a 2 výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

(5) V souvislosti s využíváním služeb informační společnosti, a aniž je dotčena směrnice 2002/58/ES, může subjekt údajů uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací.

(6) Jsou-li osobní údaje zpracovávány pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, má subjekt údajů, z důvodů týkajících se jeho konkrétní situace, právo vznést námitku proti zpracování osobních údajů, které se ho týkají, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.[149]

Právo nebýt předmětem automatizovaného individuální rozhodování

Nejedná se o nové právo, bylo součástí Zákona o ochraně osobních údajů, a to konkrétně ustanovení §11 odstavec 6:

„Žádné rozhodnutí správce nebo zpracovatele, jehož důsledkem je zásah do právních a právem chráněných zájmů subjektu údajů, nelze bez ověření vydat nebo učinit výlučně na základě automatizovaného zpracování osobních údajů. To neplatí v případě, že takové rozhodnutí bylo učiněno ve prospěch subjektu údajů a na jeho žádost.“[150]

[149] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 21
[150] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §11(6)

Jiří Žůrek uvádí ve své publikaci Praktický průvodce GDPR konkrétní příklad:

„*Není možná praxe, kdy by byla automaticky zaslána pokuta o přestupku na základě automatizovaného rozhodování, které by dnes bylo například v oblasti silniční dopravy jednoduše uskutečnitelné – kamera zaznamená vozidlo překračující povolenou rychlost, automaticky registrační značku porovná s registrem vozidel a tiskárna automatizovaně vytiskne rozhodnutí o přestupku, které linka zabalí a odešle bez lidského posouzení.*[151]

Naproti tomu automatizované individuální rozhodování Nařízení GDPR umožňuje, pokud je nezbytné k plnění či uzavření smlouvy mezi subjektem údajů a správcem údajů. Dále je umožněno, pokud s tím subjekt údajů souhlasí, nebo pokud to umožňuje právo EU či členského státu.[152] Opět Žůrek uvádí příklad z praxe: *„o automatizované posouzení půjde při zkoumání bonity žadatele o úvěr.“*[153]

Právo podat stížnost u dozorového úřadu

Pokud má subjekt údajů podezření, že zpracováním jeho osobních údajů je porušeno Nařízení GDPR, a pokud nejsou dotčeny jiné prostředky správní nebo soudní ochrany, má každý subjekt právo podat stížnost u dozorového úřadu zejména v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení.[154]

Dozorový úřad, kterému byla stížnost podána, informuje stěžovatele o pokroku v řešení stížnosti a o jeho výsledku, jakož i o možnosti soudní ochrany podle článku 78.[155] Pokud dozorový úřad odmítl nebo zamítl stížnost, stěžovatel se může obrátit na soudy ve svém členském státě.

[151] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 148
[152] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 22
[153] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018. s. 148-149
[154] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 77(1)
[155] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 77(2)

Právo na účinnou soudní ochranu

Subjekt údajů má právo na účinnou soudní ochranu vůči dozorovému úřadu, které nalezneme v článku 78 Nařízení GDPR, respektive vůči správci údajů nebo zpracovateli které je v článku 79 téhož nařízení.

Článek 78

Právo na účinnou soudní ochranu vůči dozorovému úřadu

(1) Aniž je dotčena jakákoli jiná správní či mimosoudní ochrana, má každá fyzická nebo právnická osoba právo na účinnou soudní ochranu proti právně závaznému rozhodnutí dozorového úřadu, které se jí týká.

(2) Aniž je dotčena jakákoli jiná správní či mimosoudní ochrana, má každý subjekt údajů právo na účinnou soudní ochranu, pokud se dozorový úřad, který je příslušný podle článků 55 a 56, stížností nezabývá nebo pokud neinformuje subjekt údajů do tří měsíců o pokroku v řešení stížnosti podané podle článku 77 či o jeho výsledku.

(3) Řízení proti dozorovému úřadu se zahajuje u soudů toho členského státu, v němž je daný dozorový úřad zřízen.

(4) Je-li zahájeno řízení proti rozhodnutí dozorového úřadu, kterému předcházelo stanovisko nebo rozhodnutí sboru v rámci mechanismu jednotnosti, dozorový úřad toto stanovisko nebo rozhodnutí předloží soudu.[156]

Článek 79

Právo na účinnou soudní ochranu vůči správci nebo zpracovateli

(1) Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.

(2) Řízení proti správci nebo zpracovateli se zahajuje u soudů toho členského státu, v němž má daný správce nebo zpracovatel provozovnu. Řízení se může, popřípadě zahájit i u soudů členského státu, kde má subjekt údajů své

[156] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 78

obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.[157]

Právo na zastoupení subjektů údajů

Toto právo je definováno v článku 80 Nařízení GDPR, a to tak, že subjekt má právo pověřit neziskový subjekt, organizaci nebo sdružení, které byly řádně založeny v souladu s právem některého členského státu, jejichž statutární cíle jsou ve veřejném zájmu a které vyvíjejí činnosti v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů, aby jejich jménem podal stížnost, uplatnil práva uvedená v článcích 77,78 a 79 Nařízení a, pokud tak stanoví právo členského státu, uplatnil právo na odškodnění podle článku 82 Nařízení GDPR.

„*Členské státy mohou stanovit, že jakýkoliv subjekt organizace nebo sdružení uvedené v odstavci 1 tohoto článku má bez ohledu na pověření od subjektu údajů právo podat v daném členském státě stížnost u dozorového úřadu příslušného podle článku 77 a vykonávat práva uvedená v článcích 78 a 79, pokud se domnívá, že v důsledku zpracování byla porušena práva subjektu údajů podle Nařízení GDPR.“*[158]

Právo na náhradu újmy a odpovědnost

Toto právo je definováno v nařízení GDPR jako článek 82:

(1) Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.

(2) Správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené tímto nařízením konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.

[157] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 79
[158] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 80

(3) Správce nebo zpracovatel jsou odpovědnosti podle odstavce 2 zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

(4) Je-li do téhož zpracování zapojen více než jeden správce nebo zpracovatel, nebo správce i zpracovatel, a nesou-li podle odstavců 2 a 3 odpovědnost za jakoukoliv škodu způsobenou daným zpracováním, nese každý správce nebo zpracovatel odpovědnost za celou újmu, tak aby byla zajištěna účinná náhrada újmy subjektu údajů.

(5) Jestliže některý správce nebo zpracovatel zaplatil v souladu s odstavcem 4 plnou náhradu způsobené újmy, má právo žádat od ostatních správců nebo zpracovatelů zapojených do téhož zpracování vrácení části náhrady, která odpovídá jejich podílu na odpovědnosti za újmu v souladu s podmínkami v odstavci 2.

(6) Soudní řízení za účelem výkonu práva na náhradu újmy se zahajují u soudů příslušných podle práva členského státu uvedeného v čl. 79 odst. 2.[159]

Právo odvolat souhlas

V článku 7 Nařízení GDPR je stanoveno, že „*…subjekt údajů může svůj souhlas kdykoliv odvolat, odvoláním není dotčena zákonnost zpracování vycházející ze souhlasu do doby před odvoláním. Před udělením souhlasu bude subjekt informován o možnosti odvolání souhlasu a zachování zákonnosti před jeho odvoláním. Odvolání souhlasu musí být stejně snadné jako poskytnutí.“*[160]

Oznamovací povinnost ohledně opravy, výmazu nebo omezení zpracování

Váže se na práva z nadpisu, pro něž je společné ustanovení článku 19 Obecného nařízení: „*Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s článkem 16, čl. 17 odst. 1 a článkem 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené*

[159] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 82
[160] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 7

úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.“

Zásady zpracování osobních údajů podle Nařízení GDPR

Nařízení GDPR ve svém článku 5 představuje těchto 7 zásad zpracování osobních údajů*:* „

- *Zákonnost, korektnost a transparentnost,*
- *účelové omezení,*
- *minimalizace údajů,*
- *přesnost,*
- *omezení uložení,*
- *integrita a důvěrnost*
- *odpovědnost“*[161]

Nařízení GDPR je postaveno na dvou přístupech, jedním z nich je princip odpovědnosti správce a tím druhým je přístup založený na riziku.

Princip odpovědnosti správce

Tento princip znamená odpovědnost správce za dodržení zásad zpracování osobních údajů, které jsou výše uvedeny a zároveň povinnosti správce tento soulad doložit. Tento doklad bude moci správce doložit na základě kodexu podle článku 40 Nařízení GDPR, osvědčení podle článku 42 Nařízení GDPR, certifikace, tu Nařízení nijak nezmiňuje a případně záznamy o činnostech zpracování dle článku 30 Nařízení GDPR.[162]

Princip založený na riziku

Podle názoru českého Úřadu pro ochranu osobních údajů: „*Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext*

[161] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 5
[162] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 32

a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů. V užším slova smyslu můžeme hovořit o přístupu založeném na riziku jako o aplikaci některých povinností pouze v případě, kdy zpracování osobních údajů či porušení zabezpečení (bezpečnostní incident) představuje riziko či vysoké riziko pro práva a svobody fyzické osoby. V tomto rozsahu princip založený na riziku se uplatňuje zejména u nových povinností; ohlašování, respektive oznamování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, respektive subjektu údajů, posuzování vlivu zpracování na ochranu osobních údajů a povinné konzultace s Úřadem pro ochranu osobních údajů, jejichž aplikace je vázána na přítomnost rizika či vysokého rizika pro práva a svobody fyzických osob.“[163]

Zákonnost, korektnost a transparentnost

Osobní údaje musí být ve vztahu k subjektu zpracovány zákonným způsobem, korektně a transparentně.

Zákonnost znamená, že zpracování musí probíhat v souladu s právními předpisy. Aby se tak mohlo dít zákonným způsobem, musí tak probíhat na základě souhlasu dotčené osoby, nebo na základě jiného důvodu uvedeného v článku 6 odstavec 1 písmena b) – f) Nařízení GDPR:

- *„zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
- *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
- *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*
- *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
- *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají*

[163] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 32

přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“[164]

Ke zpracování musí docházet také takovým způsobem, aby byl pro dotčenou osobu předvídatelný.[165]

Korektnost můžeme obecně definovat jako povinnost ohleduplnosti a tím i zpřísnění zásady přiměřenosti. Odpovědná osoba by měla zohledňovat zájmy a očekávání dotčeného a nesmí je bezdůvodně přehlížet nebo využívat mylných představ dotčených osob.[166]

Transparentnost vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Tato zásada se především dotýká informování subjektů údajů o totožnosti správce a účelech zpracování a o dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k dotčeným fyzickým osobám a jejich práva získat potvrzení a práva na sdělení zpracovávaných osobních údajů, které se jich týkají.[167]

Účelové omezení

Tato zásada je známa jak v evropském, tak tuzemském právu. Doplňuje právě zásadu transparentnosti a znamená, že musí být znám účel zpracování osobních údajů již při sběru dat. Pozdější změna účelu, popřípadě jeho rozšíření je možné, pouze pokud to není neslučitelné s účelem původního záměru a je pro to zákonný podklad. Ze zásady účelového omezení existují tři výjimky. První je souhlas dotčené osoby, druhou je právní předpis unijního nebo národního práva, kde to dovoluje pro cíle uvedené v Nařízení GDPR v článcích 23 odstavec 1 a 6 odstavec 4. Poslední je zpracování v souladu s archivačním zájmem, respektive

[164] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 6 (1) písm. b – f
[165] Rozsudek Evropského soudního dvora ve věci C-465/00
[166] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 39
[167] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 40

vědeckými nebo historickými výzkumy nebo statickým účelem podle článku 5 odstavec 1 písmeno b) Nařízení GDPR.[168]

Minimalizace údajů

„Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovány.“[169]

Z toho plyne, že data musí být pro sledovaný účel podstatná, musí pro tento účel být potřebná, tudíž omezená na nutnou míru odpovídající sledovanému účelu a za třetí musí být takové omezení přiměřené.

Přesnost

„*Osobní údaje musí být přesné a v případě potřeby aktualizované. Musí být přijata taková opatření, aby nepřesné údaje s přihlédnutím k účelům byly bezodkladně vymazány, popřípadě opraveny.“*[170]

Omezení uložení

„Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu a pro dané účely, pro něž jsou zpracovány, v praxi se jedná o právo subjektu být zapomenut.“[171]

To znamená, že osobní údaje mohou být uloženy pouze po dobu, po jakou je nutná identifikace osoby v souladu s účelem zpracování. Pokud uchovávání osobních údajů dané osoby již není potřebné pro daný účel, musí být tyto údaje smazány nebo musí být znemožněna identifikace osoby. Výjimky jsou pouze v případě veřejného zájmu.[172]

[168] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 40-41
[169] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 5(1) písm. c)
[170] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 5(1) písm. d)
[171] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; Článek 5(1) písm. e)
[172] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 43

Příklad: **Integrita a důvěrnost**

„Osobní údaje musí být zpracovány tak, aby byla zajištěna přiměřená bezpečnost. To znamená i ochranu před neoprávněným nebo nezákonným zpracováním a před nezamýšleným ztracením, zničením nebo poškozením dat.“[173]

Proto je zde i povinnost přijmout technická opatření podle článku 32 Nařízení GDPR: „

(1) *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:*

a) *pseudonymizace a šifrování osobních údajů;*
b) *schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;*
c) *schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
d) *procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*

(2) Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

(3) Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

(4) Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má

[173] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 5(1) písm. f)

přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.“[174]

Integrita v této souvislosti znamená ochranu nedotknutelnosti údajů. Nikdo je nemůže neoprávněně změnit, případně vymazat. Důvěrnost směřuje k ochraně dat před jejich neoprávněným zjištěním a tím i zpracováním.

Tato zásada musí být zajištěna předně vhodnou technikou, aby se nemohlo stát, že třetí osoba bude mít k datům přístup ani vhodný přístroj, kterým by mohla data zjistit a tím i zpracovávat.[175]

Odpovědnost

Zásada odpovědnosti je chápána jako zajištění dodržování zásad stanovených nařízením. K tomu patří povinnost dodržování těchto zásad prokázat.[176] Odpovědná osoba musí přijmout technická a organizační opatření, aby zajistila a doložila, že zpracovávání osobních údajů probíhá v souladu s Nařízením GDPR. Tím neodpovídá za výsledek, ale musí přijmout opatření, aby porušení Nařízení GDPR zamezila. Tyto opatřené u nás kontroluje Úřad pro ochranu osobních dat.[177]

[174] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 32
[175] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 43
[176] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 5(2)
[177] NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018 s. 44

7) Významné rozdíly

7.1. Osobní údaj

Rozdíl v pojmu osobní údaj mezi úpravou v Zákoně o ochraně osobních údajů a Obecným nařízením nenajdeme. Obě tyto úpravy pojednávají o osobních údajích naprosto totožně.

Osobní údaj je podle Zákona o ochraně osobních údajů: „ *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“.*[178]

Podle Nařízení GDPR je: *„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. “*[179]

7.2. Citlivý osobní údaj

V Zákoně o ochraně osobních údajů nalezneme definici takzvaných „citlivých údajů“, kdežto v Obecném nařízení najdeme jejich taxativní výčet pod názvem „zvláštní kategorie osobních údajů“. Jsou téměř totožné, až na údaj o odsouzení za trestný čin. Ten Nařízení upravuje samostatně ve svém článku 10.

Citlivý osobní údaj dle Zákona o ochraně osobních údajů: „*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*

[178] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písm. a)
[179] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 4(1)

subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů,"[180]

Zvláštní kategorie osobních údajů podle Nařízení: „…*vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby."* 181

Rozdíl vidím v tom, že v nařízení se nepovažuje za kategorii zvláštních osobních údajů osobní údaj o národnostním původu, který byl v Zákoně považován za osobní údaj citlivý. Za ten je naopak nově považován údaj o sexuální orientaci, který rozvíjí již v Zákoně uvedený citlivý údaj o sexuálním životě.

Zákon považoval za citlivý genetický údaj subjektu údajů. Pokud jde o biometrický údaj subjektu údajů, ten považoval za citlivý, pokud umožňoval přímou identifikaci nebo autentizaci subjektu údajů. Nařízení řadí do zvláštní kategorie osobních údajů zpracování genetických a biometrických údajů, jsou-li zpracovány za účelem jedinečné identifikace fyzické osoby (příkladem může být DNA nebo biometrický otisk prstu).

Zákon považoval za citlivý údaj o odsouzení za trestný čin, nikoliv údaj o spáchání přestupku nebo čistý trestní rejstřík. Nařízení údaj o spáchání trestného činu nepovažuje explicitně za zvláštní kategorii osobních údajů. V článku 10 ale výslovně stanovuje, že zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů se může provádět pouze pod dozorem orgánu veřejné moci nebo je-li oprávněné dle práva EU nebo členského státu. Jakýkoliv souhrnný rejstřík trestů může být veden jen pod dozorem orgánu veřejné moci, které se v tomto případě vyžadují de facto stejné povinnosti jako na zpracování zvláštních kategorií osobních údajů. V ostatních prvcích nedošlo ke změně charakteru a kontinuita jejich „citlivého" charakteru tak byla zachována.[182]

[180] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §4 písm. b)
[181] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; článek 9(1)
[182] ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018.

7.3. Fotografie zaměstnanců v osobním spise

Zákon o ochraně osobních údajů ani Nařízení GDPR v tomto ohledu nepřináší změny. Stále platí ustanovení §84 Nového občanského zákoníku:

„Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.“[183]

Nařízení GDPR ve svém recitálu 51 říká:

„Zpracování fotografií by nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby. Tyto osobní údaje by neměly být zpracovávány, pokud není zpracování povoleno ve zvláštních případech stanovených tímto nařízením, a to se zohledněním skutečnosti, že v právu členských států mohou být stanovena zvláštní ustanovení o ochraně údajů s cílem přizpůsobit uplatňování pravidel tohoto nařízení za účelem dodržení zákonné povinnosti nebo splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Společně se zvláštními požadavky na takové zpracování by se měly uplatňovat obecné zásady a další pravidla tohoto nařízení, zejména pokud jde o podmínky pro zákonné zpracování“[184]

Podle Lucie Staňkové se dle Nařízení GDPR fotografie osoby může zpracovávat na základě těchto tří právních titulů: oprávněný zájem (velký počet zaměstnanců, tak pro jejich rozeznání); právní povinnost (služební průkazy například policie); souhlas (externí použití fotografie zaměstnance na webové stránky firmy).

---

s.54;55

[183] Zákon č.89/2012 Sb., Občanský zákoník; §84

[184] Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; Recitál 51

Bartík ve své publikaci z roku 2013 Ochrana osobních údajů v aplikační praxi uvádí:

„*V praxi jsou fotografie nejčastěji uchovávány zaměstnavatelem za účelem vydání služebního průkazu, tak z hlediska Zákonu o ochraně osobních údajů se jedná o zpracování dle §5 odstavec 2 písmeno a), tedy zpracování nezbytné pro dodržení právní povinnosti správce, tedy zaměstnavatele.*[185] *V tomto případě není vyžadován souhlas zaměstnance, naopak pokud se jedná o pracovní místo vyžadující služební průkaz, má zaměstnanec povinnost zaměstnavateli fotografii poskytnout, ten ji ale může použít jen pro stanovený účel.*“

7.4. Zásady Nařízení a povinnosti podle Zákona o ochraně osobních údajů

Jak zásady Nařízení, tak i povinnosti dle Zákona o ochraně osobních údajů jsem již uvedl v předchozích kapitolách, proto nyní přistoupím pouze ke srovnání.

Obecné nařízení obsahuje zásady, které byly zavedeny na různých místech už v Zákoně o ochraně osobních údajů, tudíž by pro pečlivé správce, neměl být větší problém se zavedením Nařízení, protože výše uvedené povinnosti již plnili.

V ustanovení §5 odstavec 2 respektive §9 Zákona o ochraně osobních údajů jsou vymezeny právní důvody zpracování osobních údajů, respektive citlivých údajů. Pouze na jejich základech šlo založit legální zpracování osobních údajů a tím vlastně vidíme **zásadu zákonnosti**, kterou nám stanovuje Nařízení v článku 5 odstavci 1.[186]

Zásada korektnosti a zásada transparentnosti je upravena zase v ustanovení §11 Zákona o ochraně osobních údajů, která dává subjektu údajů právo na informace při shromažďování osobních údajů. Dále pak v ustanovení §12, kde je upraveno právo na přístup subjektu údajů k jeho osobním údajům.

[185] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(2) písm. a)
[186] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(2) a §9 ve spojení s Nařízením EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5(1) písm. a)

V ustanoveních §5 odstavec 1 písmeno g) Zákona o ochraně osobních údajů a v §5 odstavec 1 písmeno h) jsou stanoveny povinnosti otevřeně shromažďovat údaje respektive nesdružovat údaje získané k různým účelům.[187]

Zásada omezení účelu povinností správce v ustanovení §5 odstavec 1 písmeno f) Zákona o ochraně osobních údajů je povinnost zpracovávat osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny.[188]

Zásada přesnosti ta je vyjádřena v ustanovení §5 odstavec 1 písmeno c) Zákona na ochranu osobních údajů a stanovuje správci povinnost zpracovávat pouze přesné údaje, které získal v souladu s tímto zákonem.[189]

Zásada omezení uložení je povinností správce podle §5 odstavec 1 písmeno e) Zákona o ochraně osobních údajů, zde je stanovena povinnost uchovávat osobní údaje pouze po dobu nezbytně nutnou pro naplnění účelu zpracování.

Ustanovení §20 odstavec 1 Zákona o ochraně osobních údajů dále stanovuje správci či zpracovateli na pokyn správce povinnost zlikvidovat osobní údaje, pominul-li účel, pro který byly na základě důvodné žádosti subjektu údajů dle §21. [190]

Zásadu integrity a důvěrnosti lze nalézt v ustanovení §13 Zákona o ochraně osobních údajů, který upravuje povinnosti správce ohledně zabezpečení osobních údajů.[191]

[187] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §11; §12; §5(1) písm. g) a §5(1) písm. h) ve spojení s Nařízením EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5 odst. 1 písm. a)

[188] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5 (1) písm. f) ve spojení s Nařízením EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5(1) písm. b)

[189] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; § 5 (1) písm. c) ve spojení s Nařízení EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5 odst. 1 písm. d)

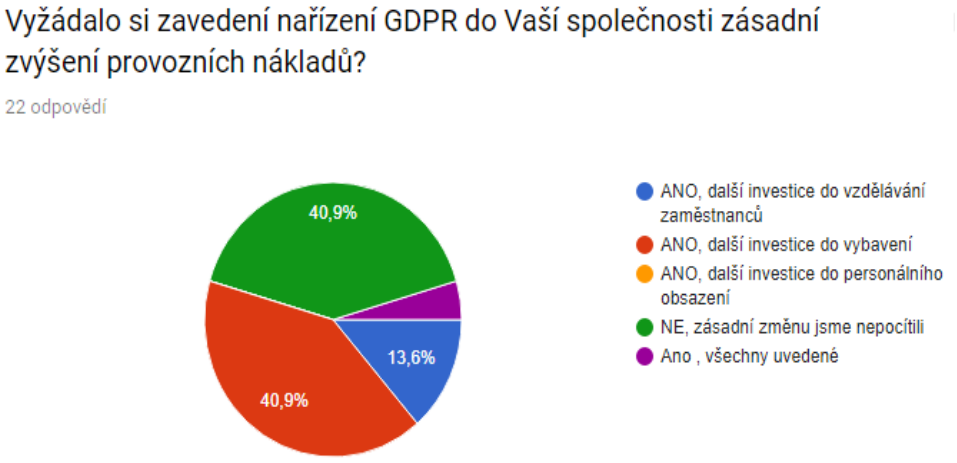
[190] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §5(1) psím e) a §20(1) ve spojení s Nařízením EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5 odst. 1 písm. e)

[191] Zákon č. 101/2000Sb., Zákon o ochraně osobních údajů; §13 ve spojení s Nařízením EU č. 2016/679 Obecné nařízení o ochraně osobních údajů; čl. 5 odst. 1 písm. f)

8) Vyhodnocení dotazníkového šetření

Pro praktickou část této diplomové práce byla zvolena metoda dotazníkového šetření s důrazem na to. jaké změny s sebou přineslo Obecné nařízení mezi různými zaměstnavateli. Dotazník byl rozesílán elektronicky a byl koncipován jako uzavřené otázky s případnou možností doplnění vlastního názoru. Za vybrané firmy dotazník zodpovídali primárně správci osobních údajů či personalisté.

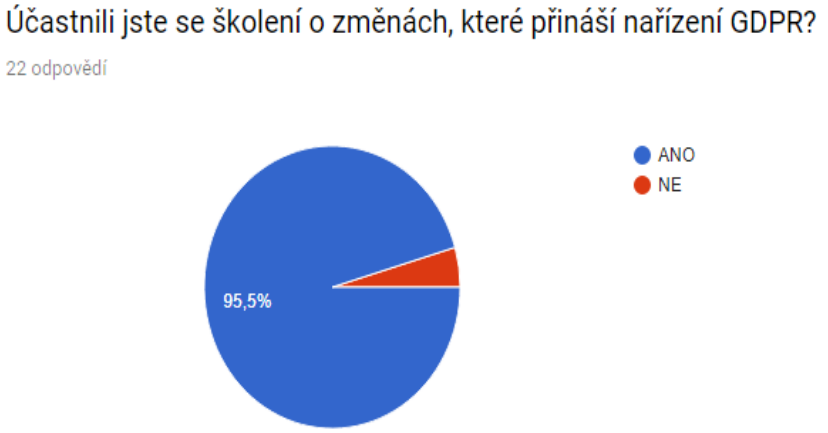
Hned v mé první otázce mě zajímalo, jaké z hlediska praxe, byly pro oslovené společnosti největší překážky při aplikaci Nařízení GDPR do firemních procesů. Při studování Nařízení GDPR jsem popravdě čekal, že největší nárůst bude buď v personálním obsazení, z hlediska vzniku funkce Pověřence pro ochranu osobních údajů, nebo v investici do vzdělávání zaměstnanců. Jak se ukázalo, tak nejvíc firmy investovali do nového vybavení, z čehož plyne, že firmy potřebovaly hlavně zkvalitnit po technologické stránce svoje dosavadní systémy uchovávání osobních údajů. Zřejmě firmy pod hrozbou vysokých sankcí zpřísnili



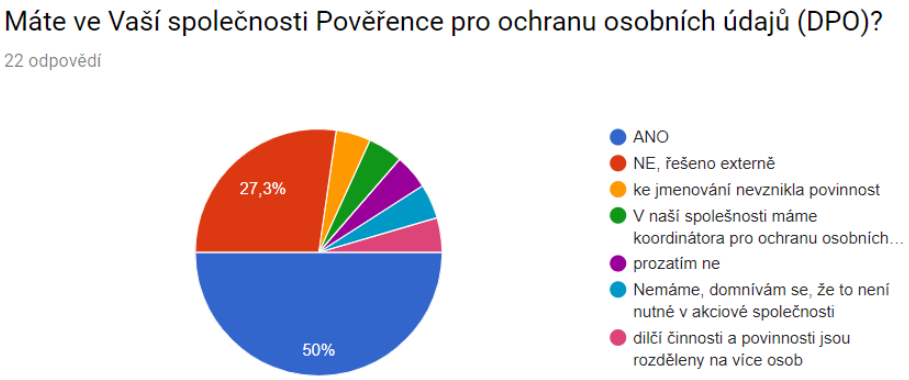
opatření na uchovávání osobních údajů

Ve druhé otázce jsem se zaměřil na to, jak firmy připravovaly svoje zaměstnance ohledně Nařízení GDPR, tedy zda před zavedením Nařízení GDPR pořádaly oslovené firmy nějaké speciální vzdělávací akce a školení. Výsledek

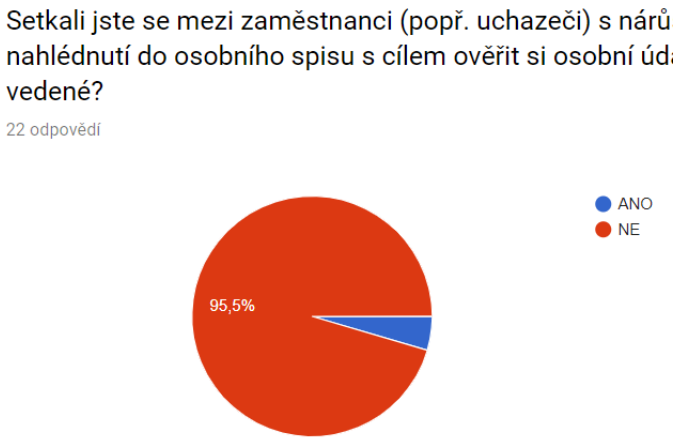
dopadl v souladu s mým předpokladem, tedy s převahou pozitivních odpovědí. Byť jsem nevěřil, že školení pro svoje zaměstnance bude pořádat více jak 95 % oslovených firem, vnímám toto rozhodnutí o proškolení velmi pozitivně a kvituji, že vybrané firmy se na aplikaci nového nařízení zodpovědně připravovali, byť to pro ně jistě znamenalo jisté náklady na vzdělávání či na kapacity zaměstnanců.



V další otázce jsem se zaměřil na nově vzniklou funkci Pověřence pro ochranu osobních údajů. Pozice, která vzniká Nařízením GDPR a není přímo potřebná pro všechny firmy. Zajímalo mne, kolik firem si samo určilo DPO, a byla jich přesná polovina z oslovených. Na druhém místě si firmy zvolily externí řešení na základě smlouvy o poskytování služeb několik firem DPO nedisponuje, jelikož nespadají do kategorie dle článku 37 Obecného nařízení, nebo mají počet zaměstnanců menší než 250, tudíž nemají povinnost vést záznamy o činnostech zpracování.

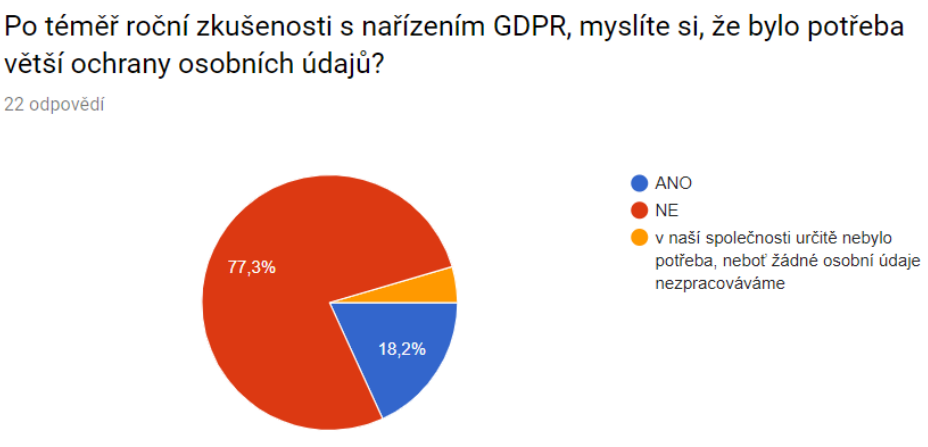


Následně jsem zjišťoval, kolik samotných zaměstnanců se rozhodlo po zavedení Nařízení GDPR zkontrolovat osobní údaje, které o nich vede jejich správce. Byl jsem překvapen, že, oproti mému původnímu předpokladu, byl jen v jedné firmě nárůst zájemců o přístup právě k těmto informacím. Hlavním důvodem by dle mého názoru mohla být nedostatečná informovanost o možnostech a právech plynoucí z Nařízení GDPR mezi zaměstnanci anebo jejich důvěra ve zpracovatele osobních údajů, že dělají svoji práci zodpovědně a pečlivě,



a s ní úzce související nepotřebnost či nezájem o ověřování si o sobě evidovaných údajů v registru zaměstnavatele.

V poslední otázce jsem se ptal na názor správců osobních údajů, zdali bylo dle jejich názoru potřeba zavádět Nařízení GDPR. Přes 80 % respondentů si myslí, že předchozí úprava uvedená v Zákoně o ochraně osobních údajů byla dostatečná. Já s nimi úplně nesouhlasím, myslím si, že Nařízení, byť hrozbou vysokých sankcí nutí správce a zpracovatele osobních údajů k větší zodpovědnosti s takovými údaji pracovat a v dnešní době, kdy jsou informace cennou komoditou, je potřeba se o ně obzvlášť pečlivě starat.



9) Závěr

Cílem mojí práce zde bylo využít mezidobí po zavedení Obecného nařízení a před jeho implementací v tuzemském právním řádu pomocí Adaptačního zákona, a porovnat Nařízení s právní úpravou uvedenou v Zákoně o ochraně osobních údajů. Zaměřuji se na důvody proč, byla nutnost zavedení Obecného nařízení, které je platné pro všechny členské státy Evropské unie. Příkladem může být mobilita pracovní síly – zaměstnanec německé národnosti může očekávat stejné nakládání s osobními údaji u nás jako ve své vlasti. Dále bylo mým cílem poukázat na místa, ve kterých se tyto právní předpisy rozcházejí, a která mají společné. Ve stručném popisu ukazuji hlavní aspekty těchto právních předpisů, povinnosti správců a zpracovatelů a zásady zpracování osobních údajů. Novinky, které přináší Obecné nařízení, jako je výše sankcí, kontroly osobních údajů ve firmách prováděny dozorčím úřadem, kterým je u nás Úřad pro ochranu osobních údajů. V dotazníkovém šetření jsem poté zkoumal vliv Nařízení na chod firem, jejich připravenost, informovanost a investice spojené se zavedením Obecného nařízení.

Cílem práce bylo právě ono srovnání a zjištění o informovanosti ve vybraných firmách a zjištění, jak se dle Nařízení změnilo nakládání s osobními údaji a údaji citlivými, respektive údaji zvláštní kategorie. Zkoumal jsem změny ve výše zmíněných pojmech, společně s tím, jestli nastali změny, co se týče fotografií zaměstnanců a jak byly zásady zpracování upraveny v Zákoně o ochraně osobních údajů respektive Nařízení. Dalším z cílů bylo zjištění investic firem po zavedení Nařízení, kde byly nuceny udělat největší finanční zásah.

Cíl jsem z větší části splnil, zjistil jsem pomocí dotazníkového šetření údaje o informovanosti správců a zpracovatelů údajů, pomocí obou úprav jsem porovnal povinnosti správců a zásady zpracování, kde jsem byl překvapen, že veškeré zásady zpracování byly různě začleněny už v Zákoně o ochraně osobních údajů. Co se týká změn okolo fotografií zaměstnanců, tak ty nedoznaly žádné změny, z čehož jsem byl také velmi překvapen, ale tento problém je patřičně definován už v Občanském zákoníku a Zákon o ochraně osobních údajů jen upravuje, za jakých podmínek má zaměstnavatel právo fotografii žádat. Zjistil jsem, že rozdíl takřka nepoznaly ani základní pojmy osobní údaj a citlivý údaj, respektive osobní údaj zvláštní kategorie. Osobní údaj byl dle mého názoru dostatečně definován už v Zákoně o ochraně osobních údajů a Nařízení definici

pouze přebralo. Na druhou stranu název citlivý osobní údaj byl nahrazen osobním údajem zvláštní kategorie a mírně pozměněn. V Nařízení je uveden jako citlivý údaj sexuální orientace, který dříve nebyl a zároveň z něj, oproti dřívějšku mizí národnostní aspekt. Nařízení dále upravuje zvlášť citlivý údaj o odsouzení za trestný čin v článku 10.

V dotazníkovém šetření jsem oslovil 22 firem napříč soukromým sektorem, které vyplněním dotazníku pomohly k vzniku této diplomové práce. Odpovídali převážně správci či zpracovatelé osobních údajů popřípadě personalisté. Čekal jsem největší narůst v oblasti personálního zastoupení, ale více než dvě pětiny oslovených firem nepocítili zásadní změnu se zavedením Nařízení, stejně velká část poté musela vložit větší množství finančních prostředků do technického vybavení. Dle mého očekávání drtivá většina firem investovala do proškolení svých zaměstnanců, kteří pracují s osobními údaji, ale takhle velký počet jsem nečekal. Otázka pověřence pro ochranu osobních údajů pro mě byla velkou neznámou, protože povinnost zřídit si DPO dle článku 37 mi nepřišla zcela určitá. Nakonec přesná polovina oslovených firem disponuje vlastním pověřencem pro ochranu osobních údajů a více než čtvrtina tuto povinnost řeší pomocí externí služby na základě smluvních vztahů. Co mi zarazilo, byl malý zájem zaměstnanců zjistit si osobní údaje o své osobě, které zpracovává zaměstnavatel. Jen v jediném případě se personalista setkal s nárůstem zájmu o nahlédnutí do svého spisu. V páté otázce se svým názorem s více než třemi čtvrtinami správců, zpracovatelů a personalistů nesouhlasím. Podle nich byla dostatečná úprava o ochraně osobních údajů již tak velmi kvalitní dle Zákona o ochraně osobních údajů a nového Nařízení tedy nebylo potřeba. Já si naopak myslím, že zkvalitnění ochrany osobních údajů u všech správců je krok vpřed v této problematice, dále pak si myslím, že v rámci globálního myšlení je v konečném důsledku v oblasti pracovního práva lepší, že, víme, co můžeme očekávat v jiných členských státech Unie při práci v jednom z nich.

10) Summary

The subject of my thesis is called Personal data protection in the labor law. This specifically theme is based on how the employer is processing with the personal data of the employees. In this thesis I wanted to show you how it was before the General Personal Data Regulation, how is the GDPR changing or not changing selected topics and in the end in the questionnaire, I examine the major impact of the GDPR on chosen companies.

I am going to show you how is this theme based on the Czech legislative and how it differs from the European regulation. I point on the main differences, especially how is personal data described in the Czech personal data protection law and in the European regulation and I point out the difference between these two legislations. For example, the sexual orientation or the criminal conviction is going to be discussed as well as issues regarding with photos of employees. However; there was absolutely no change and it is still based on the Civil code and the Regulation has the same needs as a Czech legislation. I was a bit surprised that all the processing policy has already been included in the Czech legislation in the form of the obligations.

In the final part of the thesis, I am going to present results of a questionnaire via which I would like to evaluate the impact that the regulation on questioned companies had. In the first question I deal with an issue whether the companies had (or not) to invest more because of the Regulation. Over 40% had to invested in the technological equipment. However; vice versa, the same amount of companies had no extra investment of money because of the Regulation. Another thing I was interested in was how many companies have sent their employees to the conferences or trainings about GDPR. I expect that the majority of the companies have however I did not realize that it would be over 95% of them. In the third graph you can see that a half of the asked companies have their Data Protection Officer, 6 of them have an extern DPO by contract and the rest of the companies has no duty to have one. In the next question I was seeking how the employees are curious about the personal data which their employer possesses with. And as you can see there was only one company where the employees were asking more than before the Regulation. In the final question I wanted to know the opinion of the processors, controllers and HR managers of the companies about

whether the regulation was needed for personal data protection or not. As you can see in the last graph over three-quarters of them think that it was not needed. I have different opinion and find it fruitful to have a regulation which is the same for the whole European Union because when you work in another state of the Union you can expect that with your personal data it would be handled on the same way as in your homeland.

11) Seznam literatury

Knižní publikace

BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 2. vydání, Praha: Linde Praha 2010

BARTÍK Václav; JANEČKOVÁ Eva. *Ochrana osobních údajů v aplikační praxi. Vybrané otázky. Praktická právní příručka.* 3. vydání, Praha: Linde Praha 2013

KUČEROVÁ, Alena., NOVÁKOVÁ, Ludmila., FOLDOVÁ Vanda. et al. Zákon o ochraně osobních údajů. Komentář. Praha: C. H. Beck, 2012

NAVRÁTIL Jiří a kolektiv. *GDPR pro praxi*. Plzeň nakladatelství Aleš Čeněk 2018

STAŇKOVÁ Lucie. *GDPR snadno a přehledně.* 1. vydání. Praha; Mladá fronta 2018

ŽŮREK Jiří. *Praktický průvodce GDPR.*2. aktualizované vydání. Olomouc;ANAG, 2018.

Internetové zdroje

DOLEČEK Marek. Ochrana osobních údajů – citlivé údaje. [online] 6. 2018 [cit. 23. 3. 2019] dostupná z: https://www.businessinfo.cz/cs/clanky/ochrana-osobnich-udaju-ppbi-51068.html#!&chapter=4

MAĎAROVÁ Helga. První pokuty za porušení GDPR jsou na světě. [online]. 27. 2. 2019 [cit. 26. 3. 2019]. Dostupné z: https://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-*GDPR*-jsou-na-svete-108915.html

TESAŘ Jan. Balanční test- GDPR. [online]. 2019 [cit. 22. 3. 2019]. Dostupné z: http://www.guard7.cz/gdpr/balancni-test-gdpr

Úřad pro ochranu osobních údajů. Ochrana osobních údajů na pracovišti. Příručka pro zaměstnance [online]. 2014 [cit. 21. 3. 2019]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=12691

Úřad pro ochranu osobních údajů. Zvláštní kategorie osobních údajů (citlivé údaje). [online] 5. 3. 2018 [cit. 20. 3. 2019]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaju-citlive-udaje/d-27274/p1=4744

Úřad pro ochranu osobních údajů. Právní důvody zpracování. [online]. 2018 [cit. 25. 3. 2019]. Dostupné z: https://www.uoou.cz/pravni-duvody-zpracovani/d-27318/p1=3938

Úřad pro ochranu osobních údajů. Kodexy chování [online]. 2018 [cit. 25. 3. 2019]. Dostupné z: https://www.uoou.cz/kodexy-chovani/d-29493/p1=4818

ŽŮREK Jiří. Kontrola automaticky neznamená udělení pokuty. [online]. 2018 [cit. 26. 3. 2019]. Dostupné z: https://www.uoou.cz/kontrola-automaticky-neznamena-udeleni-pokuty/d-31861

Právní předpisy

Listina základních práv EU, 2012

Listina základních práv a svobod, 1993

Nařízení Evropského parlamentu a Rady 2016/679, 2016, které pojednává o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

Občanský zákoník, 2012

Směrnice Evropského parlamentu a Rady 95/46/es, 1995, která pojednává o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

Zákon o ochraně osobních údajů, 2000

Zákoník práce, 2006

Zákon o rejstříku trestů, 1994

Zákon o zaměstnanosti, 2004

Soudní rozhodnutí

Rozsudek Soudního dvora EU ze dne 20. května 2003, ve věci c-465/00, Rechnungshof v. Österreichischer Rundfunk

Články v odborných časopisech

BARTÍK Václav; JANEČKOVÁ Eva. Fotografie v osobním spisu zaměstnance. *Práce a mzda.* 2012 č. 9