UNIVERZITA PARDUBICE

Fakulta ekonomicko-správní

Zabezpečení osobních údajů v podniku

Bakalářská práce

2021 Jakub Holeček

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Holeček**
Osobní číslo:	**E18733**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Ekonomika a provoz podniku**
Téma práce:	**Zabezpečení osobních údajů v podniku**
Zadávající katedra:	**Ústav podnikové ekonomiky a managementu**

Zásady pro vypracování

Cíl práce: Bezpečnost osobních údajů je v posledních letech neustále ohrožována především jejich dostupností prostřednictvím různých technologií. V práci budou definovány a charakterizovány osobní údaje a následně bude provedeno testování dostupnosti vybraných osobních údajů z různých organizací. Využity budou webové stránky organizací a e-mailová komunikace. Na závěr práce vyhodnotí, zda jsou zveřejňovány osobní údaje v souladu s příslušnou právní úpravou v ČR.

Osnova:
Bezpečnost osobních údajů
Právní úprava
Testování dostupnosti
Vyhodnocení výsledků

Rozsah pracovní zprávy: **35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť. ISBN 978-80-7478-139-1
JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1
BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vyd. Praha: Linde, 2013. Praktická právnická příručka. ISBN 978-80-86131-96-2
D'AMBROSOVÁ, Hana. *Ochrana osobních údajů při vedení personálních agend*. Praha: Pragoeduca, 2002. ESO. Sešity mzdových účetních a personalistů. ISBN 80-7310-003-7

Vedoucí bakalářské práce: **Ing. Pavel Jirava, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2020**
Termín odevzdání bakalářské práce: **30. dubna 2021**

L.S.

prof. Ing. Jan Stejskal, Ph.D.
děkan

doc. Ing. Marcela Kožená, Ph.D.
vedoucí ústavu

V Pardubicích dne 23. září 2020

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne

Jakub Holeček

PODĚKOVÁNÍ

Rád bych tímto poděkoval vedoucímu své práce, panu Ing. Pavlu Jiravovi Ph.D, za jeho pomoc, věcné rady a připomínky při zpracování této bakalářské práce. Dále bych chtěl také poděkovat zástupcům podniků, které za poskytnuté informace.

ANOTACE

Tato bakalářská práce je zaměřena na téma zabezpečení osobních údajů zaměstnanců vybraných podniků. Cílem práce je charakterizování osobních údajů a možné způsoby jejich využívání v podnicích. Následně bude provedeno testování jejich dostupnosti u různých organizací za pomocí jejich webových stránek a e-mailové komunikace. Závěr práce obstará porovnání dostupných údajů s právní legislativou.

KLÍČOVÁ SLOVA

Osobní údaje, podnik, GDPR, zabezpečení.

TITLE

Security of personal data in the company

ANNOTATION

This bachelor thesis is focused on security of personal data of employees in selected companies. The aim of the thesis is to describe personal data and possible manners of their using in companies. Subsequently there will be implented testing of their availability in selected companies on their websites and by e-mail conversation. The conclusion of the work will provide comparison of available data and the legislation.

KEYWORDS

Personal data, company, GDPR, security.

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

odst.	odstavec
písm.	písmeno
tzv.	takzvaný
s.	strana
ZP	Zákoník práce
FO	fyzická osoba
GDPR	Obecné nařízení o ochraně osobních údajů
WP 29	Pracovní skupina pro ochranu osobních údajů

ÚVOD

Osobní údaje jsou zvláštním druhem unikátního vlastnictví, který má každý člověk. Nemůže ho prodat, nemůže ho darovat, není možné mu ho odcizit. Jen za různých, přesně specifikovaných podmínek, část z nich může používat i někdo jiný než ten, jehož se dotýkají.

Autor se v této práce zaměřuje na zabezpečení osobních údajů v podniku. Začíná obecným přiblížením tématu ochrany osobních údajů a poté přijde blíže ke vztahu tohoto tématu na úrovni podniků a zacházení se zaměstnanci.

Prvním úkolem, bylo objasnit význam pojmů, které jsou s problematikou osobních údajů spjaty. Bude vysvětleno například o co se jedná, když se mluví o osobních údajích a udělám takový úvod do problematiky, aby byl následující text srozumitelný.

Důležitou částí bude druhá kapitola, kde budou popsány nejdříve právní důvody zpracování neboli proč někdo smí zpracovávat osobní údaje nějaké fyzické osoby. Dále pokračuji k zásadám, které musí zpracování splňovat a nastíním práva, které mají fyzické osoby, které jsou subjektem osobních údajů a kapitol ukončím tématem školení o zabezpečení osobních údajů a je zde zodpovězena také zásadní otázka. Proč je vlastně důležité osobní údaje zabezpečovat? Kdo a jak z jejich vlastnictví může profitovat.

Třetí kapitola už přiblíží téma osobních údajů do prostoru podniku. Konktrétně zde dojde k popisu, kdy a jak se ve vztahu podnik – zaměstnanec řeší téma ochrany osobních údajů, v jakých situacích vůbec je nutné toto téma vzít v potaz a při tom i jak by v praxi mělo probíhat, aby onen postup splňoval veškeré právní předpisy.

V dalším úseku dojde na problematiku využívání moderních technologií, které bezesporu přináší mnoho pozitivního pro chod a prosperitu podniku. Při jejich použití v monitoringu, je však třeba myslet na osobní údaje zaměstnanců, kterých se tato činnost dotýká.

Když byli nastíněny všechny okruhy, kterým jsem se chtěl teoreticky věnovat, zajímalo mě, jak ono nakládání s osobními údaji probíhá v praxi. Pokusil jsem se tedy oslovit některé zaměstnavatele a zjistit co nejvíce o jejich přístupu k zacházení s daty o zaměstnancích. Druhá věc, která byla zkoumána, bylo používání osobních údajů na veřejně dostupných webových stránkách od malých podniků až po nadnárodní organizace. Veškeré získané informace jsem zhodnotil, a tím zakončil svou bakalářskou práci.

1. Vymezení pojmů

Pro dobré pochopení je určitě potřeba jasné ohraničení a definování základních pojmů, se kterými budu nadále pracovat. Věřím, že dobré vysvětlení na začátku pomůže předejít možným nejasnostem a pomůže v orientaci při dalším zkoumání tématu.

1.1. Co jsou osobní údaje

Pojmem osobní údaje jsou dle stávající směrnice z roku 1995 i podle GDPR definovány jako „veškeré informace vztahující se k identifikované, či identifikovatelné fyzické osobě“ (Úřad pro ochranu osobních údajů, c 2013). Můžeme mezi ně počítat například jméno a příjmení, adresa bydliště, telefonní číslo, pohlaví, věk, datum narození a další. Je zajímavé, že to, co je pro jednu osobu osobním údajem, v případě někoho jiného být nemusí. Dobrým příkladem toho je emailová adresa. Pro někoho kdo užívá emailovou adresu jméno.příjmení@gmail.com se nejedná o osobní údaj, ale v případě jméno.příjmení@firmaxy.cz ano. Rozdíl je v tom, že první uvedený příklad může vlastnit spoustu možných lidí, pravděpodobně stejného jména, ovšem v druhém případě se dá osoba konkrétně identifikovat, protože se předpokládá, že by v jednom podniku pracovali dva lidé stejného jména a příjmení. Zásadní tedy je, zda se dá podle údajů označit konkrétní osoba (Frank Bold Advokáti, 2018).

Naopak se o osobní údaje nejedná, pokud je k identifikaci osoby potřeba nepřiměřené množství času, úsilí nebo materiálních prostředků (Hana D´Ambrosová, 2002)

Osobní údaje se dají různě rozdělovat, kupříkladu do těchto čtyř skupin na:

- Osobní údaje vedoucí k přímé identifikaci fyzické osoby
- Údaje vedoucí k nepřímé identifikaci fyzické osoby
- Další údaje
- Citlivé osobní údaje

Do první skupiny spadají takové informace, které dokážou jednoznačně určit konkrétní osobu. Dobrým příkladem by bylo rodné číslo, číslo občanského průkazu, ale také příjmení nebo bydliště. Údaje vedoucí k nepřímé identifikaci, jak již název napovídá, zahrnují takové informace, jejichž účelem je identifikace, avšak nelze pomocí nich fyzickou osobu identifikovat přesně. Zde bych uvedl jako příklad IP adresu, nebo email. Nelze totiž s úplnou

jistotou určit, kdo zrovna danou IP adresu využívá. Třetí skupinou jsem zvolil Další údaje, které jsou o fyzické osobě shromažďovány. Sem se řadí zbylé popisné informace, za předpokladu, že díky nim lze opět určit totožnost fyzické osoby. Nelze tedy říci, že by sem patřily všechny zbylé popisné informace, které nezapadají do předešlých skupin. Pokud existuje propojení, jímž se dá zjistit například že váha 73 kilogramů odpovídá panu Novákovi, o osobní údaj patřící do této skupiny se jedná. Citlivé osobní údaje jsou specifickou skupinou a věnuji jim další podkapitolu, kde je rozeberu podrobněji. Ve stručnosti se jedná o takové údaje, jenž mohou z jakéhokoliv důvodu zapříčinit diskriminaci dotyčné osoby (22 Hlav, 2017).

Další zvláštní kapitolou, která patří do tématu je pojem Biometrický osobní údaj. Tím se rozumí určitá charakteristika fyzických či fyziologických znaků osoby s jejíž pomocí je možná jedinečná identifikace. Může se jednat například o snímek obličeje, otisk prstu, snímek oční duhovky, nebo sítnice, podpis, či hlas. Biometrické údaje patří podle GDPR mezi osobní údaje zvláštní kategorie a platí zákaz jejich zpracování bez výslovného souhlasu subjektu údajů, ale existují samozřejmě i výjimky, které definuje článek 9, odstavec 2. GDPR

(Eprávo.cz, 2019).

1.2. Subjekt údajů

Subjekt údajů, nebo také Identifikovatelná osoba, je podle nařízení GDPR jakákoliv živá fyzická osoba, kterou je možné pomocí různých dat přímo, či nepřímo identifikovat.

GDPR se nevztahuje na jakékoliv právnické osoby, ale ani na zesnulé. Ovšem je třeba zmínit, že některé osobní údaje zemřelé osoby se mohou být osobními údaji i pozůstalých. Nelze opomíjet například genetickou dědičnost některých onemocnění, či předpokladů, a to se vztahuje tedy i na příbuzné dané osoby, a i když jde jen o pravděpodobnost, jedná se o jejich osobní údaj (Eprávo.cz, 2018).

Informace o právnické osobě, tedy třeba nějakém podniku nejsou osobním údajem, nevztahuje se na ně ochrana, ale údaje o zaměstnancích toho daného podniku již jsou předmětem a jsou také hlavním tématem mé bakalářské práce.

1.3. Správce a zpracovatel osobních údajů

Správce osobních údajů je ten, kdo stanovuje záměr, proč se shromažďují a zpracovávají osobní údaje, určuje, jakým způsobem budou zpracovány a nese zodpovědnost za veškeré

nakládání s nimi. V podniku jím bude bude zaměstnavatel (Hana D´Ambrosová, 2002, s. 10)

Správce odpovídá za:

- Dodržování zásad zpracování
- Zabezpečení údajů
- Dodržování povinností dle nařízení

Role správce osobních údajů může být i sdílená, potom se bude jednat o možnost společných správců, kdy nakládají s osobními údaji dva nebo více subjektů. Ty si musí rozdělit povinnosti a musí být všichni uvedeni v informacích o ochraně soukromí. Společní správci buďto pracují se společnými údaji, nebo používají údaje toho druhého. Data zpracovávají jiným způsobem pro shodné účely, nebo stejným způsobem pro jiné účely (GDPR.cz, 2018).

Zpracovatel vykonává zpracování dat jménem správce a v souladu se zadáním. Jedná se obyčejně o takzvanou třetí stranu, neboli o někoho nezávislého na podniku, jehož data zpracovává. Může to být fyzická osoba, právnická osoba, nebo orgán veřejné moci. Správce se zpracovatelem uzavírají smlouvu, ve které jsou konkretizovány povinnosti zpracovatele a další náležitosti stanovené článkem GDPR. Mimo jiné musí být ve smlouvě uvedeno, jak bude naloženo s daty po ukončení smlouvy. Když si společnost nechává vypočítávat pro zaměstnance mzdy firmou zabývající se mzdovým účetnictvím, je tato firma právě zprostředkovatelem údajů (Evropská komise, -). Ovšem ve vztahu k vlastním zaměstnancům bude firma zabývající se účetnictvím správce osobních údajů. Je tedy možné být správcem i zpracovatelem. Zpracovatel může zapojit do zpracování dalšího zpracovatele, jedná se potom o tzv. řetězení zpracovatelů, je k tomu ovšem nutné písemné svolení správce.

1.4. Zvláštní kategorie osobních údajů

Existují údaje, které mají takovou vlastnost, že dokážou sami o sobě subjekt poškodit, ať už ve společnosti, ve škole, v podnikání, v zaměstnání, nebo mohou zapříčinit jeho diskriminaci. A proto je vymezena taxativní skupina údajů, které mohou být pro subjekt citlivé, a na něž se vztahují mnohem přísnější podmínky pro zpracování. Do této speciální kategorie spadají údaje o rasovém či etnickém původu, politických názorech, náboženském, nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, o sexuální orientaci, o trestních deliktech a pravomocném odsouzení osob a patří sem také genetické a biometrické údaje, pokud jsou zpracovávány za účelem identifikace fyzické osoby. Náboženské vyznání není myšleno jako

příslušnost ke konkrétní církvi, stejně tak pro politické názory není důležité spojení ke konkrétní straně, podstatnou je především myšlenka. Pouze informace o tom, že někdo byl odsouzen za trestný čin, nebo spáchal přestupek je citlivý osobní údaj, nikoliv však informace o čistém trestním rejstříku, nebo probíhajícím trestním stíhání (Bartík, Janečková, 2013, s. 159).

Kdy je možné citlivé osobní údaje zpracovávat:

- *Subjekt údajů vyslovil výslovný souhlas*
- *Zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení, a sociální ochrany*
- *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*
- *Zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt*
- *Zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů*
- *Zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů*
- *Zpracování je nezbytné z důvodu významného veřejného zájmu*
- *Zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.*
- *Zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků*
- *Zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely*

(Úřad pro ochranu osobních údajů, 2017)

Pro většinu zmíněných kategorií platí obecný zákaz zpracování v zaměstnaneckém vztahu, ale jak později dovysvětlím, existují zde výjimky. Především co se týká informacích o zdravotním stavu, biometrických údajů, nebo i majetkových poměrech a třeba trestní bezúhonnosti. Záleží často na povaze práce. Některé citlivé údaje má zaměstnavatel dokonce povinnost zpracovávat.

1.5. Anonymizované a pseudoanonymizované údaje

Dokázat rozlišovat tyto dva pojmy je důležité především kvůli tomu, abychom dokázali správně rozpoznat, jak je možné s nimi nakládat.

Anonymizovanými osobními údaji, se rozumí takové údaje, které byly zpracovány takovým způsobem, že již není možné přesnou osobu identifikovat, a to ani nepřímo. Další podmínkou anonymizovaných osobních údajů, je že se musí jednat o anonymizaci nezvratnou (Evropská komise, c 2004).

V důsledku znemožnění propojení dat a konkrétních osob se tedy již nejedná o osobní údaje. Díky tomu je možné s nimi zacházet volněji, protože nepodléhají přísným regulím. Nejčastěji se můžeme setkat s využitím anonymizovaných osobních údajů při různých výzkumech, kdy jsou důležitá získaná data, ale už méně důležitá totožnost respondentů.

Mezi anonymizační techniky patří Randomizace a Generalizace. Randomizace spočívá v přerušení spojitosti mezi údajem a osobou, jde o úplnou náhradu, v pro účely dat nedůležitých osobních údajích. Generalizace funguje na principu zobecňování. Jsou vhodná zejména pro velké množství dat. Na příkladu data narození by fungovalo uvést říjen 1997, pokud by šlo o vzorek celé republiky, ale už nikoli, pokud by se jednalo o zaměstnance malého podniku (Eprávo.cz, 2020).

Rozdíl mezi anonymizovanými a pseudoanonymizovanými údaji spočívá v tom, že oproti první probírané skupině, kde šlo o nezvratný proces anonymizace bez možnosti zpětné identifikace, pseudoanonymizace je proces anonymizace návratné. To znamená, že došlo k zašifrování dat, tak aby podle nich nebylo možné identifikovat osobu, ale někdo pořád vlastní klíč ke zpětné dešifraci a obnovení dat. Pseudoanonymizované údaje se považují nadále za osobní údaje a ochrana se na ně dále vztahuje, kvůli možnosti zpětné identifikace (Evropská komise, c 2004).

Nejčastějšími technikami pseudoanonymizace jsou Šifrování a Hashování. Šifrování je metoda, kdy se pomocí nějakého klíče přiřadí namísto dat jiné hodnoty, a později se dají stejným klíčem dešifrovat zpět původní data. Oproti tomu Hashování je funkce pouze jednosměrná. Hash by neměl jít převést zpátky na původní hodnoty (Eprávo, 2020).

2. Zpracování osobních údajů

„Zpracování osobních údajů je jakýkoliv úkon nebo soubor úkonů, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky“ (GDPR.cz, -). Z definice vyplývá, že zpracováním osobních údajů není každá činnost s osobními údaji, ale že správce, či zpracovatel koná za určitým účelem. Mezi činnosti zpracování se řadí především shromažďování, zaznamenávání, řazení, uspořádávání, ukládání informací, zpřístupňování, pozměňování, úprava, použití, předávání, šíření, zveřejňování, uchování, výměna, třídění, výmaz, nebo likvidace (GDPR.cz, -).

2.1 Právní důvody zpracování osobních údajů

Kdyby správce neměl oprávnění ke zpracování osobních údajů, tak by postupoval nezákonně a musel je zlikvidovat. Rozhodné pro určení právních důvodů je účel zpracování dat. Pro každý účel zpracování os. údajů je potřeba mít oprávnění (Úřad pro ochranu osobních údajů, 2019).

Právními důvody zpracování osobních údajů podle (Úřad pro ochranu osobních údajů, 2019) jsou:

- *Souhlas subjektu*
- *Plnění smluvního závazku*
- *Plnění právní povinnosti*
- *Ochrana životně důležitých zájmů*
- *Veřejný zájem*
- *Oprávněné zájmy*

2.1.1 Souhlas

Článek 4 odst. 1 bod 11 Obecného nařízení definuje souhlas takto: „*Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle, který subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů*“. Tyto náležitosti by podle GDPR měl být správce schopen doložit, pokud je zpracování založeno právě na souhlasu. Subjekt by měl být obeznámen, nejen se zpracováním, jakých informací dává souhlas, ale také za jakým účelem budou zpracovávány. Subjekt také může svůj souhlas

odvolat, a pokud je to pro zpracovatele jediný důvod pro zpracování údajů, musí je zlikvidovat (Navrátil, 2018, s. 115).

2.2 Zásady

Obecné nařízení GDPR přineslo zásady, kterými by se měli správci a zpracovatelé osobních údajů řídit. Jedná se o povinnosti, za jejichž porušení hrozí udělení i vysokých pokut.

2.2.1 Zásada zákonnosti, korektnosti a transparentnosti

První zásada uvádí, že ke zpracování údajů, je vždy potřeba mít nějaký z důvodů, které jsem vyjmenoval v předchozí kapitole. Pokud zákonný důvod přestane být účinný, je nutné osobní údaje zlikvidovat. Zásada zákonitosti také znamená, že stejně jako nařízení o ochraně osobních údajů musí vyhovovat i ostatním zákonům, například není v rozporu s občanským zákoníkem. Tato zásada staví do výsadního postavení subjekt údajů, který by měl minimálně vědět, jak se nakládá s jeho údaji, v lepším případě o tom sám rozhodovat. Transparentnost v tomto případě souvisí s tím, že zpracovatel zpracovává údaje k tomu účelu, a tím způsobem, jak bylo se subjektem dohodnuto. Zpracovatel také nesmí spojovat údaje o subjektu získané pro různé účely. Tím by mohl porušovat práva subjektu, protože by ze spojení rozdílných údajů mohly vyplynout nové osobní údaje, na jejichž vlastnictví nemá správce ani zpracovatel právo (Janečková, 2018, s. 3)

2.2.2 Zásada účelového omezení

Druhá zásada je vlastně popsána již v předchozí podkapitole s názvem Právní důvody zpracování osobních údajů. Osobní údaje je možné zpracovávat pouze pro konkrétní účely. Není možné nejdříve na základě různých účelů shromáždit osobní údaje a poté je libovolně využívat. Údaje smí být zpracovány, pouze pro účel, ke kterému byly získány.

2.2.3 Zásada minimalizace údajů

Zásada minimalizace osobních údajů nařizuje správce požadovat pouze údaje, které jsou k danému účelu nezbytné. Správce by měl být schopen obhájit, k jakému účelu každý ze získaných údajů nezbytně potřebuje. Účelem tedy je stav, kdy bude správce operovat s co nejmenším počtem údajů (Janečková, 2018, s. 7)

2.2.4 Zásada přesnosti

Nesmí se stát, že by osobní údaje byly nepřesné. Správce je povinen údaje aktualizovat, pokud je to nezbytné. Mít neustále přesná a aktualizovaná data je v podstatě skoro nemožné, na správci tedy je, aby alespoň přijal veškerá rozumná opatření, aby nepracoval s nepřesnými

údaji. Pokud je zjištěno, že jsou údaje nepřesné, měly by být co nejrychleji vymazány nebo opraveny. Chyby, se kterými se můžeme setkat můžou být překlepy při zpracování, nebo i nesprávné informace jako například uvést, že byl zaměstnanec trestaný, když nebyl (Janečková, 2018, s. 8).

2.2.5 Zásada omezení uložení

Zásada omezení uložení řeší, jak dlouho si smí správce osobní údaje ponechat. Odpovědí je pouze po dobu, která je nutná k účelu jejich zpracování. O konkrétní délce té doby většinou rozhoduje sám správce, pokud není jinak zákonem stanovena.

2.2.6 Zásada integrity a důvěrnosti

Pro tuto zásadu je klíčovým ochrana osobních údajů před veškerými hrozbami. Zabezpečení se týká papírové i automatizované podoby údajů. Údaje musí být zabezpečeny technicky i organizačně před neoprávněným zpracováním, úniky informací, ztrátou, či zničením.

2.2.7 Zásada odpovědnosti

Zásada odpovědnosti nebývá uváděna pokaždé ve všech výčtech zásad. Určuje, že zodpovědnost za dodržování všech pravidel a povinností nese správce osobních údajů a zároveň je povinen tuto skutečnost doložit (Janečková, 2018, s. 9).

2.3 Práva

Stejně jako povinnosti pro správce a zpracovatele jsou stanovena práva subjektu údajů. V následujícím textu bude popsáno, jak vypadají práva subjektů osobních údajů podle úpravy GDPR.

2.3.1. Právo být informován

Toto právo pro subjekt úzce souvisí s povinnostmi správce, a to konkrétně se zásadou přesnosti, ve smyslu že zaměstnanci sdělí po pravdě, co se bude dít s jeho údaji, a také se zásadou transparentnosti. O čem by měl správce zaměstnance (v našem případě subjekt údajů) informovat stanovuje nařízení. Roli v tom hraje, jakým způsobem k nim správce přišel. Způsob informování by měl splňovat jistá kritéria. Byl by být stručný, srozumitelný, snadno dostupný, a zdarma k dispozici. Povinnost informovat se vztahuje také k opravě nebo výmazu osobních údajů. Tato povinnost neplatí pouze za předpokladu, že by to bylo nemožné, nebo nepřiměřeně náročné. V následující tabulce přímo ukážu, kdy existuje právo být informován (Nezmar, 2017, s. 84).

Tabulka 1: Právo být informován

Jaké informace musí být sdělovány?	**Údaje získané přímo od subjektu údajů**	**Údaje získané nepřímo od subjektu údajů**
Identifikační údaje a kontaktní údaje na správce a pověřence pro ochranu údajů	Ano	Ano
Účel zpracování a zákonné oprávnění pro zpracování	Ano	Ano
Oprávněné zájmy správce nebo případně třetí strany	Ne	Ano
Kategorie osobních údajů	Ne	Ano
Každý příjemce nebo kategorie příjemců osobních údajů	Ano	Ano
Podrobnosti o přesunech dat do třetích zemí a poskytnutých zárukách	Ano	Ano
Doba uchovávání nebo kritéria používaná k určení doby uchovávání	Ano	Ano
Zdroj, od kterého pocházejí osobní údaje	Ne	Ano
Zda je poskytování osobních údajů součástí zákonného nebo smluvního závazku nebo požadavku a možné důsledky neposkytnutí os. údajů	Ano	Ne
Kdy mají být informace poskytnuty	V okamžiku získání dat	V přiměřené lhůtě (do 1 měsíce

Zpracováno podle: (Nezmar, 2017, s. 84)

2.3.2. Právo na přístup

Dalším právem subjektu je získat potvrzení o zpracování osobních údajů, mít přístup ke svým osobním údajům a na další doplňující informace. Tato možnost nabízí, aby si mohli zaměstnanci sami kontrolovat jaké údaje o nich zaměstnavatel zpracovává. Ověřit tak jejich

správnost a rozsah. Žádosti na přístup by mělo být vyhověno, ovšem nemusí to být zadarmo. V prvním případě ano, ale při dalších žádostech je správce oprávněn při daných podmínkách požadovat přiměřený poplatek, který bude odpovídat nákladům na poskytnutí. Po podání žádosti má správce měsíc na poskytnutí, který může prodloužit na dva měsíce, za předpokladu, že je přístup příliš složitý, musí však o tomto prodloužení žadatele včas informovat. Správce tento požadavek může i odmítnout, pokud je žádost zjevně nedůvodná nebo nepřiměřená, a to třeba tím, že je často opakovaná (Nezmar, 2017, s.85).

2.3.3. Právo na opravu

Pokud jsou osobní údaje nepřesné, nebo neúplné, mají subjekty právo na opravu. Když subjekt zažádá o opravu, musí tak správce vykonat do jednoho měsíce, případně, pokud je oprava náročná může tuto lhůtu o další dva měsíce prodloužit. O tomto prodloužení musí subjekt informovat. Pokud správce nepřistoupí k nápravě, musí podat vysvětlení proč se tak rozhodl a poučit subjekt o jeho právu podat stížnost dozorovému orgánu.

2.3.4. Právo na výmaz

Právo na výmaz, jinak také právo být zapomenut není absolutní právo. Když subjekt podá žádost, aby byly jeho osobní údaje smazány, mělo by mu být vyhoveno. Nejčastějšími důvody je odvolání souhlasu, nebo že již nejsou potřeba ke splnění účelu, anebo k nim žádný právní důvod nikdy nebyl. Naopak důvody pro odmítnutí této žádosti jsou například plnění zákonné povinnosti a další důvody, které byly vyjmenovány v podkapitole Právní důvody zpracování osobních údajů (Nezmar, 2017, s. 86).

2.3.5. Právo na omezení zpracování

Omezené zpracování znamená, že je zpracování pozastaveno, jedinou možnou operací je uložení údajů, ale nesmí se dále zpracovávat. K tomuto postupu dochází většinou pokud se zrovna něco přezkoumává. Třeba pokud se zjistí nepřesnosti v osobních údajích, a tak se nemohou nadále zpracovávat, dokud nebude chyba opravena. Dalším důvodem by bylo, kdyby zaměstnanec podal námitku proti zpracování, tak by se po čas šetření, zda je oprávněné, omezilo, pozastavilo. Posledním případem, který zmíním je případ kdy uplyne účel zpracování, ale správce si údaje může ponechat z důvodu případné právní ochrany, tak bude zpracování údajů také omezeno pouze k uložení. Poté, co skončí omezení a údaje se opět můžou začít zpracovávat, je o této skutečnosti správce povinen subjekt údajů informovat (Nezmar, 2017, s. 88)

2.3.6. Právo přenositelnosti

Právo přenositelnosti subjektu údajů umožňuje získat a znovu použít své údaje u jiného správce. Toto právo najde uplatnění především například ve službách, kde má zákazník právo bezpečně kopírovat nebo přesouvat své údaje od jednoho dodavatele ke druhému. Převedení údajů neznamená automaticky konec práva na zpracování pro původního správce (Janečková, 2018, s. 25).

2.3.7. Právo vznést námitku

Pokud není osobě umožněno plnění některého z práv, vzniká jí právo vznést námitku. První reakcí na tento krok by mělo být pozastavení zpracování. Následnou povinností správce je doložit, že důvody ke zpracování jsou pádnější, než argumenty proti, jako je právo svobody. Osoby mohou vznést námitku, pokud cítí, že jsou zpracovávány jejich údaje k účelu, ke kterému nemají správci svolení. Právo vznést námitku by mělo být obsaženo v podnikovém prohlášení o ochraně osobních údajů, a tudíž by s ním měli být zaměstnanci konkrétně obeznámeni. Speciálně se toto téma týká zpracování údajů pro účely marketingu. Pokud osoba vznese námitku proti použití svých údajů pro účely marketingu, musí jí být bezpodmínečně vyhověno a příslušná data odstraněna (Nezmar, 2017, s. 91)

2.4. Školení zaměstnanců

Nařízení GDPR nařizuje správcům a zpracovatelům povinné školení v oblasti ochrany osobních údajů. Většina útoků na osobní údaje jsou zapříčiněny lidskou chybou. Proběhlé školení zaměstnanců by mělo být zdokumentované pro doložení, že organizace udělala nezbytné kroky k souladu s nařízením a jedná v souladu s GDPR. Účastníci musí chápat veškerá rizika práce s osobními údaji, i jaké dopady by mělo jejich nesprávné použití. Je potřeba, aby bylo školení přizpůsobené danému podniku a jeho způsobům práce s údaji. Zaměstnanci by také měli být schopni rozpoznat porušení ochrany dat a vědět, a jak takovou událost hlásit. Školení by mělo probíhat průběžně, aby zahrnovalo nové zaměstnance, ale i ty stávající z důvodu měnících se nařízení, nebo technologického vývoje (Nezmar, 2017, s. 180). Podle webu elegal.cz podniky školení často opomíjejí. Podle nich se ale jakýkoliv druh školení rozhodně vyplatí. Dobrým informováním zaměstnanců snížíte riziko špatného nakládání s osobními údaji, které může vést k finančním postihům, poškození reputace, a i když už k úniku dojde, může doložení o provedeném školení přispět ke zmírnění trestu (Elegal.cz, 2019).

2.5 Proč se vlastně zabezpečují osobní údaje?

Důvodů proč chránit osobní údaje, a jaké hrozby přináší jejich únik je několik a jsou různé. Získávat cizí osobní údaje mohou chtít výrobní podniky a další obchodní organizace pro účely cílené reklamy a tím zvýšení poptávky pro jimi nabízeném produktu. Pro takové organizace mají tedy data o osobách obchodní hodnotu. Pro jiné osoby nebo organizace mohou mít cizí údaje hodnotu pro zločinecké úmysly a může vést k fyzickému napadení, jiné formě útoku, nebo okradení dotyčné osoby. Další nekalé získávání dat může sloužit k realizaci podvodů na fyzických osobách jako je krádež identity, vydírání, nebo podvodné bankovní transakce. Přístup k neoprávněným údajům ale může znamenat nebezpečí pro celou společnost, kterou by znamenala například mezinárodní špionáž (Nezmar, 2017, s. 99)

Pro podnik hrozí navíc kromě výše zmíněných hrozeb také udělení vysokých pokut, v případě, že nedokáže dobře zabezpečit osobní údaje. Pokuta může vyšplhat až do výše 10 000 000 EUR, případně 2% z celkového ročního obratu podniku, a nebo až do výše 20 000 000 EUR, či 4% celkového ročního obratu. Tyto dvě sazby jsou rozdílné podle toho, jak závažně byly porušeny povinnosti (Nezmar, 2017, s. 44).

3. Osobní údaje zaměstnance na časové ose

V této kapitole bude popsáno, jak probíhá proces zpracování osobních údajů od výběrového řízení po ukončení pracovního poměru se zaměstnancem. Rozdělím vztah zaměstnance se zaměstnavatelem do tří fází: Před vznikem pracovního poměru, během zaměstnání a po ukončení pracovního poměru a v každé fázi se pokusím vysvětlit kontext ochrany osobních údajů.

3.1 Zpracování osobních údajů před vznikem pracovního poměru

Již při prvním kontaktu potenciálního zaměstnavatele se zaměstnancem podnik začíná zpracovávat jeho údaje. Vzniku pracovního poměru předchází většinou první kroky, které představují zaslání životopisu či motivačního dopisu od uchazeče o zaměstnání. Tyto dokumenty obsahují řadu osobních údajů, a tak již zde nastává podniku povinnost řídit se podle zásad zpracování osobních údajů.

Cílem zaměstnavatele je zjistit informace o uchazečích, které mu pomohou z nich vybrat vhodného zaměstnance. Podnik potřebuje získat tolik údajů, aby byl schopen se rozhodnout pro správnou osobu, avšak je limitován řadou skutečností. Může totiž požadovat osobní informace od zaměstnanců pouze v případě, kdy bezprostředně souvisejí s uzavřením pracovní smlouvy. Na základě získaných informací se zaměstnavatel nesmí rozhodovat diskriminačně (Morávek, 2013, s. 377). Údaje, které zaměstnavatel požadovat nesmí popisuje § 12 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti „*zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu se zvláštním právním předpisem, 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“* (zákon č.435/2000 Sb). Pokud je ovšem nesporné, že požadovaný údaj z výčtu zakázaných souvisí s výkonem práce, má na jeho zjištění potenciální zaměstnavatel právo. Například pokud jde o zaměstnání vyžadující časté služební cesty, je přijatelné zjišťovat, zda má zájemce děti, protože má tento fakt přímý vliv na výkon práce (Morávek, 2013, s. 378).

Po skončení výběrového řízení se nabízí, že by data neúspěšných kandidátů měla být zničena a kandidáti s tímto krokem seznámeni. To podle Morávka ovšem není ideální řešení a měli by si ponechat část údajů do vypršení doby promlčení možných žalobních nároků. Pokud by totiž neúspěšný kandidát napadl výběrové řízení, bude podnik muset dokazovat, že se nedopustil diskriminace (Morávek, 2013, s. 377). Personalisté také často žádají o svolení k uchování údajů o uchazeči za účelem vytvoření databáze, pro další výběr zaměstnance až se znovu uvolní jiná volná pozice. Po svolení v tomto případě budou uloženy údaje do evidence potenciálních zaměstnanců na přiměřenou dobu, která by měla být zhruba 6 měsíců. To je totiž doba, za kterou uchovávání dat o potenciálním zaměstnanci ztratí smysl, protože se mohou během té doby změnit. Po uplynutí doby, pokud nebylo jinak sjednáno, nastává podniku opět povinnost údaje zlikvidovat (Bartík, Janečková, 2013, s. 157).

Zaměstnavatelé ovšem nemusí čekat na zájem uchazečů o zaměstnání, ale také je aktivně vyhledávají třeba na databázích pracovních portálů, nebo prostřednictví profesních sociálních sítí. Pokud uchazeč v rámci snahy o získání zaměstnání svolil se sdílením svého životopisu, případně své údaje vyplnil v nějakém dotazníku, správcem těchto údajů je daný portál, kterému osoba tyto materiály poskytla. Podnik je potom od ní s vědomím majitele může získat k užití jako zpracovatel. V případě, že podnik zveřejní inzerát s nabídkou pracovní pozice na pracovním portálu, bude potom správcem osobních údajů, zatímco portál se stane zpracovatelem.

Obecně lidé zveřejňují spoustu osobních údajů na svých sociálních sítích. I když jsou tyto údaje zveřejněné dobrovolně, podniky, ani nikdo jiný je nesmí bez právního důvodu zpracovávat. Jiné je to s profesními sociálními sítěmi. Takovým příkladem je sociální síť LinkedIn, která je přímo zaměřená na náborovou činnost. Uživatel při vstupu souhlasí s podmínkami služby. Fyzické osoby zde mohou vyhledávat zaměstnání, ale stejně tak mohou podniky vyhledávat ideální kandidáty na volnou pozici, pokud má daný profil zájem o nové zaměstnání (Eprávo.cz, 2018).

3.2 Zpracování osobních údajů zaměstnance

Pokud dojde k dohodě o uzavření pracovní smlouvy, okamžitě přibývají zaměstnavateli pravomoci zjišťovat další informace. Nyní může požadovat veškeré potřebné údaje pro vedení personální a mzdové agendy jako je třeba rodné číslo a také může začít zjišťovat informace, které mají souvislosti s výkonem práce, ale jejichž znalost nebyla zapotřebí k rozhodování o přijetí uchazeče, a tak na ně má zaměstnavatel nárok až nyní.

Ke sběru těchto informací obvykle slouží tzv. Osobní dotazník. Osobní dotazník je formulář, který vyplňuje nový zaměstnanec při nástupu do zaměstnání. Údaje z tohoto dotazníku může podnik použít pro vedení personálních a mzdových agend. V osobním dotazníku by se mohly objevovat otázky na identifikační údaje, kontaktní údaje, dosažené vzdělání, dosažená praxe, případně i zájmy uchazeče. Pokud je to pro vykonávání zaměstnání věcné tak třeba také informace o trestní bezúhonnosti, řidičském osvědčení, vlastní podnikatelská činnost, nebo může být také vlastnictví zbrojního pasu. Není však možné pro zjednodušení pořizování kopií osobních dokladů zaměstnance. Bez řádně opatřeného souhlasu, který by mohl zaměstnavatel po dobu držení kopie doložit se jedná o přestupek podle § 16a odst. 1 písm. K) zákona o občanských průkazech. Při získávání údajů musí mít zaměstnavatel stále na mysli zásadu minimalizace dat (Morávek, 2013, s. 382).

Některé osobní údaje je zaměstnavatel povinen shromažďovat, a to na základě několika právních předpisů. Jsou to informace sloužící k výpočtu mzdy, daní, vypočítání sociálního a zdravotního pojištění, nebo třeba pro určení data odchodu do starobního důchodu. To znamená, že zaměstnavatel pracuje třeba i s informacemi o dětech zaměstnance, ať už pro výpočet daní, nebo u žen pro určení odchodu do důchodu. Pro odvod zdravotního pojištění musí znát zdravotní pojišťovnu zaměstnance. Může se také dostat ke zdravotnímu znevýhodnění nebo státnímu občanství. Tyto informace nepřicházely v úvahu před uzavřením smlouvy. Výjimkou z pravidel je v tomto ohledu také evidence pracovních úrazů nebo nemocí z povolání. Ačkoli se jedná o citlivé údaje, zaměstnavatel je musí evidovat, a to i bez souhlasu zaměstnance (Práce a mzda, 2017).

Nemoc z povolání a pracovní úrazy nejsou jedinými citlivými údaji které zaměstnavatel musí o zaměstnancích zpracovávat. Zůstaneme ještě u informací o zdravotním stavu, což se dá považovat vždy za citlivý údaj. V některých oborech nejde zaměstnání vykonávat bez zvláštních zdravotních nebo hygienických způsobilostí. Z bezpečnostních důvodů je také nezbytné evidování těhotných pracovnic. Těhotná zaměstnankyně musí znát rizika, která by mohla mít vliv na těhotenství a zaměstnavatel musí tato rizika, včetně fyzické a psychické námahy, snížit na minimum (Bartík, Janečková, 2013, s. 176). Stejně jako je v některých oborech zapotřebí bližší znalost zdravotního stav, tak to samé platí jinde pro bezpečnost, a tak je v jiných oborech nutná znalost další kategorie citlivých údajů, týkající se trestních deliktů. Podniky, které pracují za těchto podmínek by měly ztát tyto údaje dokonce již při náborovém procesu.

Zákoník práce umožňuje vést podniku v rámci personalistiky tzv. Osobní spis zaměstnance, není to však jeho povinnost. V něm může shromažďovat písemnosti, tykající se jejich pracovněprávního vztahu jako je třeba kvalifikace, doklady související s uzavřením smlouvy, doklady o proškolování, ale mohou tam patřit také i stížnosti na daného zaměstnance. Osobní spis samozřejmě obsahuje také řadu osobních údajů (Jouza, 2018). Zaměstnavatel ho může vést jak v papírové, tak i v elektronické formě. Do Osobního spisu zaměstnance smí nahlížet orgán inspekce práce, úřad práce, soud, státní zástupce, Policie, Národní bezpečnostní úřad a zpravodajské služby. Výše uvedení mají právo na informace z osobního spisu, ne však na kompletní, ale pouze ty, které potřebují k výkonu své práce. Dále mohou nahlížet do spisu také vedoucí pracovníci, ale jen ti, kteří jsou zaměstnanci nadřízení, firemní právník a sám zaměstnanec smí nahlížet do svého spisu (Bartík, Janečková, 2013, s. 173).

Součástí osobního spisu může být také fotografie zaměstnance. Zejména ve velké organizaci, kde se zaměstnanci navzájem neznají, může zaměstnavatel používat fotografii z bezpečnostních důvodů. Portrétová fotografie je nepochybně osobním údajem, jelikož splňuje definici, že může vést k identifikaci osoby a její zpracování tedy podléhá zásadám o zpracování osobních údajů. Pokud nedochází k dalšímu zpracování, jako by bylo třeba rozdělení podle biometrických charakteristik vyplývajících z fotografií, tak se nejedná o citlivý osobní údaj. Pokud je fotografie zpracovávána pouze pro účely služebního průkazu, jedná se o plnění právní povinnosti správce a v tom případě není zapotřebí souhlas zaměstnance, naopak je jeho povinností fotografii poskytnout. V ostatních případech je zapotřebí zaměstnancův souhlas, nebo jiný oprávněný zájem (Bartík, Janečková, 2013, s. 169).

Často bývají fotografie zaměstnanců umístěné na internetových stránkách podniku, doplněné dalšími informacemi o nich a pozici, kterou vykonávají. Samotné přiřazení zaměstnance k pozici, by mohl provést podnik bez udělení souhlasu, ale pro použití fotografie a doplňkových informací o osobě je již souhlas nezbytný. Fotografie ze zaměstnaneckých akcí, které nemají za účel sloužit k identifikaci, ale zachycují zaměstnance při nějaké události nespadají pod GDPR, ale pod Občanský zákoník a souhlas k jejich zpracování stačí jakýkoliv projev souhlasu, který ovšem je i nadále odvolatelný (Podnikatel.cz, 2019).

Zajímavým osobním údajem jsou informace o příjmu fyzické osoby. Mají velmi blízko k citlivým osobním údajům. Zákon je mezi ně neřadí, i když se dá říci, že naplňují jejich podstatu, protože mohou být pro osobu velmi citlivé a mohou zapříčinit její diskriminaci ve

společnosti. Aby se jednalo o osobní údaj, musí být identifikováno, nebo alespoň identifikovatelné spojení mezi mzdou či platem a konkrétním zaměstnancem. Údaje o výši mzdy mohou, ale nemusí být součástí pracovní smlouvy. Pokud není, tak bývá stanovena v tzv. platovém výměru. V obou případech bude informace o výši příjmu součástí osobního spisu, pokud ho zaměstnavatel vede. To znamená, že k nim mají přístup nadřízení pracovníci, mají ovšem povinnost mlčenlivosti. Kromě vedoucích pracovníků si mohou vyžádat informace o výši příjmu i ostatní organizace vyjmenované v předchozím odstavci, za předpokladu, že jejich znalost souvisí s plněním jejich úkolů a dostanou je i bez svolení dotyčného zaměstnance. (Bartík, Janečková, 2013, s. 178). Naopak zaměstnavatel nemá žádné pravomoci, aby zakázal zaměstnancům mezi sebou informace o svých mzdách vyměňovat. Zaměstnanec má právo, ne však povinnost na ochranu osobních údajů, a tak když uzná za vhodné, smí se o své mzdě svěřit komu chce, nebo dát souhlas zaměstnavateli k možnosti zveřejnění svého platu k tvorbě personální politiky (BOZP info, 2018). Může také nastat situace, kdy kontaktuje zaměstnavatele finanční organizace, která poskytla nějakou formou jeho zaměstnanci půjčku s žádostí o ověření příjmu. Zaměstnavatel sám o sobě nemůže sdělovat příjmy zaměstnanců, ani potvrdit informace o jejich výši. Nejdříve by musel získat od zaměstnance svolení, bez svolení zaměstnance tyto informace nemůže poskytnout, i kdyby to bylo v jeho zájmu. Jiná situace je u údajů o platech, tedy pokud jde o zaměstnance veřejných institucí. Pokud je zveřejnění ve veřejném zájmu, může k němu dojít, je ovšem důležité poměřovat veřejný zájem s právem na ochranu soukromí. U mezd byla myšlenka, že by jejich zveřejňováním bylo možné odhalit a zabránit diskriminaci v odměňování, ovšem převážil aspekt ochrany osobních údajů (Bartík, Janečková, 2013, s. 183).

Další zpracování osobních údajů zaměstnanců probíhá při tzv. monitoringu, což je jedna z personálních činností. Zaměstnavatel může kontrolovat výkonnost pracovníků, hlídat majetek podniku, nebo tento postup může sloužit k ochraně zdraví pracovníků. Tuto činnost výrazně ovlivnil vývoj a dostupnost technologií. Konkrétní praktiky monitoringu jsou používání kamerových systémů, GPS systémů, kontrola elektronické pošty, či internetové historie. Používání těchto nástrojů ovšem logicky naráží na práva zaměstnanců. Zaměstnanec jako fyzická osoba má vždy zaručená osobní práva jako právo na soukromí a ta mají v právním měřítku vyšší hodnotu než práva podniku na ochranu majetku a zájem, aby zaměstnanec pracoval efektivně. Zaměstnavatel proto musí při monitoringu postupovat velmi opatrně a respektovat relevantní předpisy. Sledování činnosti zaměstnanců nesmí nikdy probíhat tajně, zaměstnanec o jeho možnostech musí být informován. Nástroje monitoringu

blíže rozeberu ve vztahu s technologickým pokrokem v následující kapitole (Bartík, Janečková, 2013, s. 137).

I v případě, že má zaměstnavatel z právních důvodů povinnost data zpracovávat, nesmí zapomínat všechny zásady a pravidla pro zpracování osobních údajů a také samozřejmě musí dávat zvýšený pozor, protože, některá z těchto dat mohou spadat do kategorie citlivých údajů a podle toho s nimi také nakládat.

3.3 Zpracování osobních údajů po ukončení pracovního poměru

Dalo by se očekávat, že doba zpracování osobních údajů zaměstnance bude trvat po čas pracovního poměru. Pro správce je ovšem rozhodující, jak již bylo zmíněno, účel zpracování osobních údajů, a ten může mít i po ukončení pracovního poměru. Obdobně také rozvázáním pracovního poměru nekončí veškeré právní závazky a ty s sebou také nesou zpracování osobních údajů. I po ukončení pracovního poměru může nadále platit například konkurenční doložka, může dojít ke kompenzování nevyčerpané dovolené a podobně. (Morávek, 2013, s. 387).

Dokumenty, které pozbyly účel, a tak nejsou potřeba uchovávat, jako je třeba životopis, by měly být navráceny zaměstnanci, anebo prokazatelně zničeny. Tzv. výmaz musí být nenávratný a musí proběhnout v papírové i elektronické formě, bez toho, aby o to musel dotyčný člověk zažádat. Zaměstnavatel je povinen nadále uchovávat některá data pro účel archivace. Netýká se samozřejmě všech dokumentů. Archivovat musí například evidenční nebo mzdové listy. Druhým účelem uchování dat i po odchodu zaměstnance je oprávněný zájem zaměstnavatele. To může být pro možnou potřebu důkazu ve sporu o platnosti ukončení pracovního poměru, nebo obvinění z diskriminace. I zde samozřejmě platí, že data zpracovávaná pro tento účel nesmí být využívána pro jiný účel. Lhůta pro uchování dat pro tento účel je odvozena od promlčecí lhůty (Podnikatel.cz, 2018).

Právnička Diana Schneiderová v článku na webu Podnikatel.cz zmiňuje archivační lhůty některých dokladů.

Tabulka 2: Lhůty archivace dokumentů po ukončení pracovněprávního vztahu

Evidenční listy důchodové pojištění	3 roky
Záznamy o pojistném na sociálním zabezpečení	6 let
Údaje pro účely důchodového pojištění	10 let
Mzdové listy	30 let
Doklady z oblasti nemocenského pojištění	10 let
Daňové doklady	10 let
Doklady týkající se srážek ze mzdy	30 let
Doklady o pracovněprávních náležitostech	30 let
Docházka do zaměstnání	3 roky
Výtky / pozitivní hodnocení zaměstnance	3 roky

Zpracováno podle: (Podnikatel.cz, 2018)

4. Monitoring zaměstnanců s využitím technologického pokroku

Monitoringu zaměstnanců byla částečně věnována pozornost již v rámci Zpracování osobních údajů zaměstnanců, kde jsem neměl tolik prostoru toto téma rozvádět, abych tolik nenarušil strukturu kapitoly, a protože je to rozsáhlé téma, rozhodl jsem se mu věnovat vlastní kapitolu

S tím, jak se technologie vyvíjí a modernizuje se mění také oblast osobních údajů. A jako ve většině ostatních oblastech to i zde přináší příležitosti i hrozby. V této kapitole budou rozebrány zajímavé vynálezy, ať už nové, nebo starší, které měly vliv na otázku osobních údajů a vynutily si pozornost právních úprav. Technologický pokrok v posledních letech nejspíše nejvíce ovlivňuje oblast osobních údajů zaměstnance. Ostatní pravidla, ač se třeba mění s příchodem GDPR, tak mají základy už dávno dané a moc se nemění.

4.1. Monitoring zaměstnanců

V oblasti monitoringu se střetávají práva zaměstnance, tedy fyzické osoby, se zájmy podniku. Zaměstnavatel chce kontrolovat, zda zaměstnanci pracují efektivně, chce chránit svůj majetek a také bezpečnost v podniku. Velká změna přišla především v dostupnosti různých nástrojů používaných pro monitoring.

Zaměstnanec má právo na uspokojivé pracovní podmínky a prostředí, což znamená jednak přijatelné teplo, hluk, nebo prach na pracovišti, ale také sociální podmínky a mezi ně patří i ochrana soukromí a právo vytvářet a rozvíjet mezilidské vztahy, a to i během pracovní doby. Ovšem to hlavní, čemu by se měl zaměstnanec v pracovní době věnovat, jsou jeho pracovní úkoly a zaměstnavatel tak má právo ho kontrolovat, ovšem musí tak konat přiměřeným způsobem a prostředky, s respektem k právu zaměstnance na soukromý život. Bude tedy potřeba aby se poměřovaly tato dvě protichůdná práva a kontrola byla omezená na nutnou nebo přiměřenou úroveň (Morávek, 2013, s. 66).

Tento problém nelze vyřešit vyjádřením souhlasu zaměstnavatele, protože ten by nebyl platný. Právo na ochranu soukromí, patří mezi základní lidská práva a svobody a ty nesmí být omezeny v žádném případě, ani na základě vlastního rozhodnutí dané fyzické osoby. Možnost využívat technologie monitoringu tedy závisí především na povaze pracovní činnosti (Bartík, Janečková, 2013, s. 137).

Před zaváděním nových opatření by si měl zaměstnavatel vyhodnotit tzv. test proporcionality, při kterém by měl zvážit jaké má důvody pro zavedení nového nástroje, jaký bude mít přínos, jaká data bude zpracovávat a zda jsou nutná, a na kolik to zasáhne do soukromí zaměstnance.

Dalším nutným krokem při implementování nového způsobu kontroly je řádné informování dotčených zaměstnanců. Nové nástroje také znamenají pro podnik technické i organizační zabezpečení získaných údajů před všemi druhy rizik (Právní prostor, 2019).

4.1.1 Kamery

Pořizování záběrů a záznamů pomocí kamerových systému funguje k identifikaci fyzických osob a jejich chování, tudíž se jedná o zpracování osobních údajů. Není tomu tak ovšem ve všech případech. Aby se jednalo o osobní údaje, musí být ze záznamu alespoň nepřímo identifikovatelná konkrétní fyzická osoba. Osobní údaje poté tvoří ty charakteristické znaky, pomocí jihž byla tato osoba identifikována. I když se ale nachází na záznamu osoba k jejíž identifikaci nemáme dostatečné informace, stejně se k těmto záběrům musí přistupovat jako k osobním údajům, protože se nedá vyloučit, že v budoucnosti dojde doplněním informací a následné identifikaci osob.

Kamery na pracovišti mohou sloužit k více účelům. Prvním je ochrana majetku. Kamerový systém často zamezí případným krádežím ještě předtím, než nastanou, případně po krádeži, nebo poničení majetku může pomoci objektivně odhalit pachatele. Druhým účelem, proč se zaměstnavatel rozhodne pro instalaci kamer je sledování zaměstnanců, zda důsledně využívají pracovní doby k plnění svých povinností. Dalšími důvody může být ochrana bezpečnosti v podniku, nebo kontrola správnosti technologického postupu. (Bartík, Janečková, 2013, s. 141).

Využívání kamer by mělo být až poslední variantou, před jejich zavedením by měl podnik zvážit, zda není možné docílit zmíněných účelů jinou, méně obtěžující metodou. Jak už jsem zmiňoval, zaměstnavatel nemůže jen tak sledovat své zaměstnance. Jediným důvodem, jak legálně používat kamery pro sledování zaměstnanců znamená využití výjimky dle § 316 odst. 3 ZP, který umožňuje tuto praxi v případě závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele. V jakémkoliv jiném případě se jedná o porušení ZP, protože se jedná o zásah do soukromého života zaměstnanců. Ani v případě zmíněné výjimky, ale nemůže zaměstnavatel monitorovat bez omezení. Svou důležitost také hraje umístění kamer. Je vyloučeno používání kamer např. na chodbách nebo na sociálních zařízeních, kde chybí objektivní důvod sledování.

4.1.2. Internetový prohlížeč

Zaměstnavatel má právo vymezit pravidla práce na internetu a tím klidně úplně zakázat jeho používání pro soukromé účely. Alternativou tohoto striktního zákazu je umístění některých

stránek na tzv. blacklisty a zakázat tím používání pouze konkrétních stránek. Zakázanými stránkami budou v praxi nejčastěji nejspíše sociální sítě, stránky s erotickým obsahem, hry, nebo například filmy. Řešení kontroly tohoto nařízení se nabízí dvě, buďto přístup k vybraným stránkám rovnou zablokovat, nebo provádět namátkové kontroly. Pokud není užívání internetu pro soukromé účely podnikem zakázáno, ke kontrole a jejímu rozsahu musí zaměstnavatel získat zaměstnancův souhlas (Morávek, 2013, s. 404).

Zaměstnavatel může používat řadu nástrojů pro zjišťování aktivity zaměstnanců na svěřeném majetku, v tomto případě internetovém připojení a nejspíše svěřeném počítači. Jejich využívání by však mělo být spíše nahodilé, než systematické a zaměstnanec by měl být o těchto možnostech informován.

4.1.3. Emaily

Základním orientačním právem v otázce, zda smí zaměstnavatel zaměstnanci kontrolovat elektronickou poštu spočívá z Listiny základních práv a svobod. Ta zaručuje ochranu listovního tajemství. To samé platí tedy stejně jako pro emaily například i pro SMS zprávy a další komunikační sítě. Tedy platí, že i na elektronickou poštu se vztahují stejná pravidla jako na ostatní písemnosti, které stanovuje například § 12 ObčZ. Podnik musí respektovat, že se jedná o soukromou zprávu, i když přišla jejich zaměstnanci, v jeho pracovní době, na jejich zařízení. Na rozdíl od kamerového systému, pokud dá k monitorování písemností zaměstnanec souhlas, tak k němu může docházet.

Zaměstnavatel nemá právo nikdy prohlížet zaměstnancovu soukromou emailovou adresu. O soukromé zprávy se jedná i u pracovní emailové adresy patřící zaměstnavateli, kterou má zaměstnanec zřízenou pro výkon práce na své jméno, například jmeno.příjmení@firmaxy.cz. V tomto případě by zaměstnavatel neměl mít přístup k obsahu konverzace, ale v rámci sledování využití pracovní doby zaměstnancem by mohl sledovat objem došlé a odeslané konverzace, případně jejich hlavičku, a požadovat, aby vyřizoval své osobní záležitosti během pracovní doby v minimální míře. Se záměrem tohoto druhu sledování by měl být zaměstnanec obeznámen, stejně jako by měl být ujištěn, že obsah jeho pošty je chráněn a zaměstnavatel ctí poštovní tajemství. Jiný případ jsou tzv. úřední emailové adresy, které jsou ve tvaru například info@firmaxy.cz, tak se nejedná o soukromé zprávy, i kdyby ji za podnik spravovala jen jedna osoba a tu zaměstnavatel může kompletně monitorovat.

Zaměstnavatel je oprávněn za výjimečných situací v zájmu ochrany svých práv otevřít a přečíst zaměstnancův soukromý pracovní email. Taková situace může nastat například když

je z hlavičky zřejmé, že jde o pracovní email a je nepravděpodobné, že k jeho vyřízení dojde včas, čímž by zaměstnavatel utrpěl újmu. Zaměstnavatel by potom uplatňoval právo ochránit svůj majetek. Pro předcházení takovým situacím, je vhodné dohodnout zastupování při výkonu dovolené (Bartík, Janečková, 2013, s.143).

Za konkrétních podmínek je možné nahlížet i do pracovní emailové adresy bývalého zaměstnance. Je třeba tak konat způsobem, který co nejméně zasahuje do jeho soukromí. Přečíst obsah emailu je opět možné až pokud je z hlavičky zřejmé, že se jedná o dopis pracovní povahy, se kterým by bývalý zaměstnavatel objektivně měl být seznámen. Pokud je potřeba na ten email reagovat, není možné to provést z této adresy. Při ukončení pracovního poměru je vhodné, aby sám zaměstnanec předal zaměstnavateli důležité emaily, ten je případně archivoval a účet odstranil. Postup řešení této situace by měl být popsán v interních předpisech (Eprávo.cz, 2020).

4.1.4. Služební automobil

V první řadě je důležité zmínit, že služební automobil je vlastně pracovní nástroj. Provoz firemních automobilů je velmi nákladnou položkou, a tak mají zaměstnavatelé zájem sledovat jejich provoz. Pomocí GPS systémů je možné zjistit o provozu vozidla řadu informací jako přesnou trasu jízd, nebo spotřebu pohonných hmot, rychlost vozidla, či dodržování povinných pauz u řidičů dálkové přepravy. To znamená, že s využitím GPS souvisí zpracování řady osobních údajů.

Zaměstnanci musí být informováni o instalaci těchto zařízení a datech, která budou shromažďovat. Není to ovšem jen povinnost, ale to vědomí podniku i prospěje. Pokud totiž bude zaměstnanec vědět, že má podnik k dispozici data o jeho způsobu řízení, bude si počínat šetrněji (Bartík, Janečková, 2013, s. 149).

V případě, že je umožněno zaměstnanci využívat služební vozidlo i k soukromým účelům, by mělo být možné sledovací zařízení vypnout, aby nedocházelo ke zpracování přebytečných dat.

4.1.5 Služební telefon

Při používání služebních telefonů, ať už mobilních, nebo pevné linky je stejně jako u užívání služebního vozidla důležité odlišit používání pro soukromé a pracovní účely. Opět záleží na nastavení konkrétních vztahů a pravidel pro používání svěřeného majetku. Je možné, že zaměstnavatel povolí a bude hradit zaměstnanci i soukromé hovory, nebo jim je povolí uskutečňovat, ale musí si je zaznamenávat, a jejich hodnota jim potom bude odečtena z platu.

Potom má zaměstnavatel právo provádět namátkové kontroly. Obsah hovoru je zaměstnavateli zapovězený, ale smí zjišťovat telefonní čísla, na která zaměstnanec volá, a to za účelem omezení nákladů na telefonní služby, popřípadě kontroly využití pracovní doby zaměstnancem. Pro určování telefonních čísel se dají využít různá technická zařízení. Ze samotného telefonního čísla ovšem nelze s jistotou usoudit, zda se jednalo o soukromý hovor.

Pokud bude zaměstnavatel systematicky shromažďovat údaje o zaměstnancově užívání služebního telefonu, například na jaká čísla a jak často volá, bude se jednat o zpracování osobních údajů. Tyto údaje mu mohou být užitečné při vyhodnocování, zda budou zaměstnanci dané hovory strženy z platu, což uplatní například v účetnictví. V tom případě by k tomuto jednání zaměstnavatel ani nepotřeboval souhlas, jelikož se jedná o zpracování nezbytné pro dodržení právní povinnosti (Bartík, Janečková, 2013, s. 148).

5. Zkoumání stavu ochrany osobních údajů ve vybraných podnicích

V závěrečné kapitole bude provedeno zkoumání úrovně ochrany osobních údajů zaměstnanců vybraných podniků a vyzkoušena jejich dostupnost na webových stránkách. Každou společnost nejprve krátce představím, poté uvedu, jaké osobní údaje byly nalezeny na webových stránkách firem, a nakonec se zaměřím na zkoumání prvků, které byly popsány v předchozích kapitolách. Po provedení této analýzy bude zjištěno v první řadě kolik osobních údajů svých zaměstnanců různé podniky sdílejí na internetu a poté se pokusím zodpovědět, zda podnik zpracovává veškeré osobní údaje sám, nebo některá data sdílí s externím zpracovatelem, které nástroje monitorování v podniku využívají, jak nakládají s údaji o neúspěšných kandidátech na zaměstnání a bývalých zaměstnancích a zda praktikují školení ohledně zacházení s osobními údaji. S některými společnostmi se mi podařilo navázat kontakt a dotázat se jich přímo na následující otevřené otázky:

1. Zpracovává Váš podnik veškeré osobní údaje zaměstnanců sám, nebo pro některé účely využíváte externí zpracovatele?
2. Jaké nástroje používáte v podniku k monitorování zaměstnanců?
3. Jak nakládáte s osobními údaji neúspěšných uchazečů o zaměstnání?
4. Jak nakládáte s osobními údaji bývalých zaměstnanců?
5. Probíhá u Vás v podniku školení o nakládání s osobními údaji?

Další organizace mi už v přímé komunikaci informace neposkytly, ovšem na jejich webových stránkách, se mi podařilo najít, alespoň na část otázek odpovědi, a tak jsem zpracoval jejich profil na základě těchto materiálů.

5.1 Charvát group

Firma Charvát Group s.r.o. sídlí ve Zbraslavicích ve Středočeském kraji a vznikla transformací do současné podoby v roce 2006. Své dceřiné firmy má společnost na Slovensku v Chorvatsku a na Ukrajině. Celkově zaměstnává přes 800 pracovníků a dosahuje obratu kolem 65 milionů Euro. Společnost podniká na trhu průmyslové hydrauliky. Společnost je výrobcem hydraulických válců, armovaných hadic, hydraulických trubek, dodavatelem uceleného sortimentu hydraulických komponentů jako je šroubení, rychlospojky, dodavatelem

technických řeční know-how, a je také dodavatelem průmyslových kapalin. Společnost dále provozuje vlastní nadační fond a dostihovou stáj.

Po analýze webové stránky společnosti, byly nalezeny kontaktní údaje některých specifických zaměstnanců jako například zaměstnankyni zodpovědnou za nábor uchazečů o zaměstnání v podobě jejího jména, pozice, telefonního čísla a emailové adresy obsahující její jméno. Podobné údaje je možné nalézt také o jednateli, asistentce jednatele, zaměstnancích ekonomického úseku, obchodního úseku, reklamací, expedice, výrobního úseku a také osoby odpovědné za GDPR. Některé zaměstnance je také možné identifikovat pomocí biometrických údajů, které je možné rozpoznat z propagačního videa.

Na webových stránkách lze také nalézt obsáhlé poučení o GDPR, především ve vztahu k zákazníkům, pro marketingovou a obchodní činnost. Je zde uvedena například totožnost správce údajů jako společnost Charvát Group s.r.o., je zde uvedena odpovědná osoba za ochranu osobních údajů, doba uložení osobních údajů, účel zpracování, upozornění na právo na odvolání a na přístup k osobním údajům, právo na opravu či výmaz a mimo jiné také právo na podání stížnosti. Je zde i návod, jak práva uplatnit, a to kontaktováním správce, nebo přímo odpovědné osoby na poštovní nebo emailové adrese (Charvat-chs.cz., c 2021).

Tabulka 3: Dostupné osobní údaje firmy 1

K dispozici na webových stránkách	Ano / Ne
Jména zaměstnanců	Ano
Email zaměstnance, obsahující jméno	Ano
Profilová fotografie konkrétního zaměstnance	Ne
Propagační fotografie / video obsahující zaměstnance	Ano
Životopis zaměstnance	Ne
Poučení o zpracování osobních údajů zákazníků	Ano
Poučení o zpracování osobních údajů zaměstnanců	Ne
Kontakt na správce osobních údaje (způsob řešení problémů)	Ano

Vlastní zpracování podle údajů dostupných z: (Charvat-chs.cz, c 2021)

S podnikem se autorovi povedlo navázat komunikaci formou emailové konverzace.

Na první otázku ohledně zpracování údajů dalšími zástupkyně firmy reagovala jen, že zpracovávají osobní údaje pouze v nezbytné míře pro pracovní poměr.

Další otázka byla směřována na monitoring, kde bylo zjištěno, že společnost provádí evidenci docházky a používají GPS systémy ve služebních vozech, kvůli případnému odcizení, naopak služební telefon, ani internetový prohlížeč nekontrolují.

Údaje o neúspěšných uchazečích jsou archivovány na základě jejich souhlasu po dobu maximálně šesti měsíců, poté jsou automaticky skartovány pro případ papírové podoby, v případě elektronické podoby jsou obdobně zlikvidovány a stejně tak také elektronická komunikace s potenciálními uchazeči, která je také zlikvidovaná po uplynutí šesti měsících.

Osobní údaje bývalých zaměstnanců jsou řízeny archivačním řádem společnosti, který kopíruje zákon o archiváliích. Stejně v elektronické i papírové podobě.

Další otázka směřovala na praktikování školení. Osobní údaje má ve společnosti na starosti pouze velmi omezený počet zaměstnanců a ti vzhledem ke své pracovní pozici mají zákony týkající se ochrany osobních údajů nastudovaný, a proto prý v současné době není nutné tyto zaměstnance školit.

Závěrem bylo sděleno, že se společnost na zabezpečení osobních údajů snaží velmi dbát. Listinná podoba dokladů je zabezpečena v uzamykatelných místnostech, kam mají přístup pouze příslušní pracovníci. Osobní údaje jsou používány pouze v nezbytně nutné míře pro vznik, trvání a ukončení pracovního poměru.

5.2 Parkon, s.r.o.

Zahradní centrum Parkon sídlí v Libici nad Cidlinou, na trase mezi Kolínem a Poděbrady. Podnik je rozdělen na velkoobchodní prodej vypěstovaných rostlin a travin a na maloobchod, kde také prodává vlastní vypěstované rostliny, a navíc další sortiment jako jsou ovocné stromy, jehličnany, pnoucí dřeviny, vřesovištní rostliny, balkonové a pokojové rostliny, travní koberce, substráty, hnojiva, postřiky, keramiku a další doplňkový sortiment, jako jsou třeba čaje, nebo koření. Okrasná školka se rozléhá na ploše 1,2 hektaru a vyprodukuje zhruba 80 000 kusů různých rostlin každý rok.

Podle počtu zaměstnanců se jedná o malý podnik, který zaměstnává 10 až 15 stálých zaměstnanců. Protože v tomto oboru hraje velkou roli sezónnost, využívá často také brigádníky a studenty vykonávající odbornou praxi.

V sekci kontakty na webových stránkách podniku lze nalézt pouze telefonní kontakty na oba jednatele a kontaktní emailová adresa, z níž nelze identifikovat osobu, která ji obsluhuje. K dispozici je také seznámení s bezpečností a ochranou osobních údajů zákazníků (Parkon.cz, c 2021).

Tabulka 4: Dostupné osobní údaje firmy 2

K dispozici na webových stránkách	Ano / Ne
Jména zaměstnanců	Ne
Email zaměstnance, obsahující jméno	Ne
Profilová fotografie konkrétního zaměstnance	Ne
Propagační fotografie / video obsahující zaměstnance	Ne
Životopis zaměstnance	Ne
Poučení o zpracování osobních údajů zákazníků	Ano
Poučení o zpracování osobních údajů zaměstnanců	Ne
Kontakt na správce osobních údaje (způsob řešení problémů)	Ano

Vlastní zpracování podle údajů dostupných z: (Parkon.cz, c 2021)

Autor práce dokázal navázat s podnikem kontakt prostřednictvím emailu a získal odpovědi na udané otázky.

Podnik za některými účely spolupracuje s externími zpracovateli osobních údajů, konkrétně mzdovou účetní, jíž podnik poskytuje údaje nezbytně nutné pro výkon její práce. Zaměstnanci jsou s tím obeznámeni a vyjádřili souhlas.

Areál podniku je střežen kamerovým systémem za účelem ochrany majetku a zamezení krádežím. Kamery nejsou instalovány v prostorách určených pouze pro zaměstnance, jako je například šatna, nebo kuchyňka. Emaily ani internetový prohlížeč nejsou kontrolovány.

Veškeré údaje o neúspěšných uchazečích o zaměstnání jsou neprodleně po ukončení přijímacího řízení nenávratně zlikvidovány.

V případě bývalých zaměstnanců jsou některé údaje ihned vymazány a jiné musí být podle zákona nadále archivovány. V tomto ohledu se řídí podle zákona o archiváliích.

Školení o zacházení s osobními údaji ve firmě neprobíhá.

5.3 Komerční banka, a.s.

Komerční banka je bankovní institucí, která zaměstnává přes 7 tisíc zaměstnanců, kteří v České republice obsluhují více než 1,6 milionů klientu, což je zhruba každý pátý dospělý člověk. Jedná se tedy o jednu z největších finančních institucí v zemi a také mezi největší zaměstnavatele. V roce 2019 měla banka k umístění svých zaměstnanců 343 poboček na území České republiky a významným prostředí pro ně bylo také internetové bankovnictví.

Osobní údaje zaměstnanců Komerční banky lze na internetu dohledat na dvou adresách. Jednou jsou tradičně webové stránky a tou druhou internetové bankovnictví, kam mají přístup pouze klienti banky. V rámci internetového bankovnictví má klient ať už v mobilní aplikaci, nebo v internetovém prohlížeči kontakt na svého bankovního poradce. Kontakt obsahuje informace o jménu a příjmení přiděleného zaměstnance, s jeho fotografii, obsahující biometrické údaje. Je zde také možnost dotyčnou osobu kontaktovat telefonicky, či emailovou zprávou, čímž lze zjistit emailová adresa, obsahující jméno, a telefonní číslo.

Na webových stránkách lze v sekci „Lidé v KB“ najít členy představenstva a jejich profily, které obsahují kromě jména a fotografie jejich představení formou životopisu, který obsahuje celou řadu osobních údajů. V sekci kontakty pak lze najít opět základní informace na kontaktní osoby obchodní divize pro obsluhu „top“ korporátních klientu, které obsahují shodně jméno, pozici, telefonní kontakt, emailová adresa obsahující jméno a adresu místa výkonu práce. Týká se to ovšem jen velmi úzkého okruhu zaměstnanců a většina kontaktů jsou řešena formou infolinky, nebo emailu pro celé oddělení, ne na konkrétní zodpovědné osoby.

Tabulka 5: Dostupné osobní údaje firmy 3

K dispozici na webových stránkách	Ano / Ne
Jména zaměstnanců	Ano
Email zaměstnance, obsahující jméno	Ano
Profilová fotografie konkrétního zaměstnance	Ano
Propagační fotografie / video obsahující zaměstnance	Ano
Životopis zaměstnance	Ano
Poučení o zpracování osobních údajů zákazníků	Ano
Poučení o zpracování osobních údajů zaměstnanců	Ano
Kontakt na správce osobních údaje (způsob řešení problémů)	Ano

Vlastní zpracování podle údajů dostupných z: (Kb.cz, c 2021)

Na webu Komerční banky je také k dispozici záložka Ochrana osobních údajů, která obsahuje tři podkapitoly: Ochrana osobních údajů, Kontakty, Pro zaměstnance. Z tohoto zdroje jsem částečně získal odpovědi na mé otázky.

První záložka je určena pro klienty banky. Je stručně shrnuté poučení o zpracování informací o klientech, potom jsou zde odpovědi na otázky jako:

- Kdo je správcem vašich osobních údajů a jak ho můžete kontaktovat?
- Na základě jakých zákonných důvodů jsou zpracovávány osobní údaje?
- Jak jsou získány osobní údaje?
- Kdo jsou zpracovatelé a příjemci vašich údajů?
- Jak dlouho údaje uchováváme?
- Jaká práva mají subjekty údajů?

Prostřední záložka neobsahuje kontakt na Pověřence pro ochranu osobních údajů, ale také kontakt na Úřad pro ochranu osobních údajů, odkaz na nařízení GDPR a doprovodná stanoviska WP 29.

Nejvíce přínosná záložka pro tuto práci byla záložka třetí s označením Pro Zaměstnance, kde dostanou potřebné informace o zacházení s údaji zaměstnanci, kandidáti na zaměstnání a externisté. Informace jsou zde jednak ve formě PDF souboru ke stažení, nebo rozepsané do otázek podobnou formou jako u informací pro klienty. Z materiálů jsem zjistil, že je správcem osobních údajů vždy některý ze členů Skupiny KB. Hlavní zásady jsou zpracování údajů pouze pro stanovený účel, stanovenými prostředky a způsobem, pouze po nutnou dobu vzhledem k účelu. Druhou zásadou je zabezpečení dat před neoprávněným přístupem, únikem, či zničením. A třetí zásadou je mlčenlivost osob přicházející s údaji do kontaktu. Pro zpracování údajů používají pro některé účely externí zpracovatele, ale ručí za stejné zásady, jakými se řídí sami.

Informace o zájemcích o zaměstnání jsou získávané ze zaslaných životopisů, či prostřednictvím personální agentury, na základě vzájemné komunikace, nebo ze sociálních sítí a internetu. Z internetu mohou být získány informace ze živnostenského rejstříku, obchodního rejstříku, insolvenčního rejstříku, nebo třeba sítě LinkedIn. Po uplynutí doby, po kterou je zpracování údajů potřebné pro plnění účelu jsou údaje zlikvidovány. Po udělení souhlasu za účelem případného obsazení jiné pozice mohou být uchovány po dobu 24 měsíců.

Osobní údaje zaměstnanců jsou zpracovány pro plnění tří účelů. Plnění smlouvy, Splnění právní povinnosti a Oprávněného zájmu. Pro účel Splnění právní povinnosti uchovávají údaje po dobu 30 let po skončení pracovního poměru v České republice a na Slovensku dokonce po dobu 70 let. Pro ostatní účely je ta doba kratší. Za účelem dodržování právních povinností jsou na provozovnách pořizované kamerové záznamy, u vybraných pracovních pozic dochází k monitorování také telefonických hovorů a elektronické komunikace, služební vozy jsou vybavené GPS pro odlišování služebních a soukromích cest a s cílem chránit interní dokumenty je hlídán i internetový prohlížeč. Informace o zaměstnancích jsou získávány ze vstupního formuláře, vstupního pohovoru a vzájemné komunikace, dále z aplikací využívaných při práci a z bezpečnostních systémů (Komerční banka, c 2021).

5.4 MAN Truck & Bus Czech Republic s.r.o.

Společnost MAN je německý strojírenský holding, který je zastoupený v České republice od roku 1992. Zabývá se výrobou nákladních automobilů a autobusů a dalším oblastem strojírenství jako je výroba vznětových motorů, dieselelektrických agregátů, nebo parních

a plynových turbín. Celosvětově zaměstnává okolo 35 000 zaměstnanců tato německá společnost, která většinově spadá pod koncern Volkswagen group.

V Českých pobočkách nevyrábí nové stroje, ale prodávají hotové, nebo opravují již zakoupené společně s dalšími po prodejovými službami, a to v prodejním a servisním centru v Brně, v Čestlicích u Prahy, v Rousínově na Moravě, v Ostravě a v Postřižíně.

Po prozkoumání webových stránek bylo nalezeno z osobních údajů pouze kontakt na HR managerku v podobě emailu obsahující její jméno (Manoriginal.cz, c 2021) a na druhé webové stránce společnosti opět údaj stejný kontakt, ovšem na jiného zaměstnance odpovědného za nábor a byli zde také použity fotografie zaměstnanců pro ilustraci (Man.eu, c 2021).

Tabulka 6: Dostupné osobní údaje firmy 4

K dispozici na webových stránkách	Ano / Ne
Jména zaměstnanců	Ano
Email zaměstnance, obsahující jméno	Ano
Profilová fotografie konkrétního zaměstnance	Ne
Propagační fotografie / video obsahující zaměstnance	Ne
Životopis zaměstnance	Ne
Poučení o zpracování osobních údajů zákazníků	Ano
Poučení o zpracování osobních údajů zaměstnanců	Ano
Kontakt na správce osobních údaje (způsob řešení problémů)	Ano

Vlastní zpracování podle údajů dostupných z: (Manoriginal.cz, c 2021 a Man.eu, c 2021)

Společnost na svých stránkách volně nabízí poučení o ochraně osobních údajů pro obchodní partnery i pro zaměstnance. Zaměstnancům deklaruje, že zpracování jejich osobních údajů probíhá v míře nezbytné pro dosažení dvou účelů. Prvním je realizace pracovněprávního vztahu. V tomto případě zpracovávají údaje v nezbytném rozsahu pro plnění závazků z pracovněprávního vztahu od doby nástupu po ukončení pracovního poměru. Do tohoto bodu spadá například poskytování zaměstnaneckých výhod, realizace pracovních cest, nebo zvyšování kvalifikace. S tím také souvisí, že mohou být údaje zaměstnanců poskytnuty

například zprostředkovatelům školení, zpracovateli mzdové agendy, nebo třeba poskytovateli ubytování na pracovní cestě, či jiným subjektům.

Druhým účelem je plnění právních povinností zaměstnavatele. Tyto důvody se dotýkají pracovního práva. Konkrétně se jedná například o lékařskou prohlídku, nebo odvod daní a pojištění za zaměstnance. Pro tento druh zpracování je právním důvodem některý z právních předpisu právního řádu České republiky. To znamená, že mají zaměstnanci povinnost tyto údaje poskytnout, bez nich nemohou být zaměstnáni. Údaje zpracovávány za tímto účelem mohou být poskytnuty příslušným státním úřadům a institucím, nebo poskytovateli pracovně lékařské prohlídky.

Zaměstnanci využívající služební automobil mohou být monitorováni, a jejich údaje zpracovávány za účelem komplexní evidence jízd. Základní osobní údaje mohou být předány leasingové společnosti.

Po ukončení pracovního poměru bude společnost uchovávat některé údaje z následujících důvodů:

a) Realizace důchodové agendy poživatelů starobního nebo invalidního důchodu

b) Realizace důchodové agendy

c) Ochrana před případnými právními nároky

Pro body a) a b) opravňuje společnost právní řád České republiky a údaje uchovávají v bodě a) po dobu 10 let a v bodě b) po dobu 45 let od skončení roku ukončení zaměstnání. Kvůli bodu c) se archivuje část osobního spisu, obsahující pracovní smlouvy nebo doklady dokazující podstoupení lékařské prohlídky pro dokázání, že společnost dodržela veškeré povinnosti a mohla se bránit případným právním krokům. Jedná se o oprávněný zájem a podle typu dokumentu může jeho zpracování trvat až 30, v některých případech až 100 let.

5.5 SCIO, s.r.o.

Motivací společnosti Scio je změnit svět v oblasti vzdělávání. Společnost je známa svými testy, průlomovým byl pro firmu tzv. test Obecných studijních předpokladů, který stále využívá mnoho vysokých škol jako kritérium v přijímacím řízení. Kromě testování, ale provozuje společnost nyní 11 vlastních základních škol a jednu střední školu. Dalším produktem, který nabízejí, nazývají paralelní vzdělávání, kterým pomáhají rodičům s rozvojem jejich dětí, nebo hračky podporující rozvoj dětí (Scio.cz, c 2021).

Po prozkoumání webových stránek byl nalezen kontakt pro uchazeče o zaměstnání se jménem a příjmením kontaktní osoby, její portrétní fotografie a emailu ve formě obsahující příjmení. Další kontakt obsahující stejné údaje k dispozici patří zaměstnanci odpovědnému za kontakt s médii. V sekci nazvané O nás je k popisu firmu přiložená koláž 52 portrétních fotografií zaměstnanců bez dalších údajů.

Tabulka 7: Dostupné osobní údaje firmy 5

K dispozici na webových stránkách	Ano / Ne
Jména zaměstnanců	Ano
Email zaměstnance, obsahující jméno	Ano
Profilová fotografie konkrétního zaměstnance	Ano
Propagační fotografie / video obsahující zaměstnance	Ano
Životopis zaměstnance	Ne
Poučení o zpracování osobních údajů zákazníků	Ano
Poučení o zpracování osobních údajů zaměstnanců	Ano
Kontakt na správce osobních údaje (způsob řešení problémů)	Ano

Vlastní zpracování podle údajů dostupných z: (Scio.cz, c 2021)

Tato společnost jsem byla vybrána k prozkoumání z důvodu, že na svých webových stránkách nabízí velmi obsáhle zpracované poučení o zpracování osobních údajů. Protože firma vyhodnocuje různé testy, provozuje vlastní školy, a také například provozuje e-shop s prodejem vzdělávacích hraček, zpracovává opravdu velké množství osobních údajů za různými účely a různými způsoby. Kapitolu osobní údaje mají z toho důvodu rozčleněnou do podrobnějších podkapitol a každou zvlášť přehledně vysvětlují. Nacházejí se zde obecné kapitoly věnující se vysvětlení základních pojmů o zpracování osobních údajů, zpracování citlivých osobních údajů, a práva subjektů. Dále se zde zmíněné kapitoly podle využívané služby jako jsou například Národní srovnávací zkoušky, projekty pro školy, projekty pro rodiče a děti, „hračky vzdělávačky“, a v neposlední řadě cookies a zasílání newsletterů. U jednotlivých kapitol je vysvětlen účel zpracování, jaké osobní údaje jsou zpracovávané, doba zpracování osobních údajů, právní titul zpracování osobních údajů, popřípadě předávání osobních údajů jiným subjektům.

Na stránkách se také nachází informace o zpracování osobních údajů zaměstnanců, kde jsou zodpovězeny stejné otázky, jako zákazníků, je zde uveden správce osobních údajů, jsou zde znovu nadefinované základní pojmy, a vysvětlená práva. Společnost SCIO nepoužívá žádné externí zpracovatele, a tudíž nesdílí osobní údaje zaměstnanců s nikým, vyjma příslušných úřadů, ke kterým existuje povinnost.

O uchazeči o zaměstnání podnik zpracovává údaje poskytnuté v životopise, kontaktní údaje, fotografii, pokud ji uchazeč poskytne, výsledky testu Personline, a pracovní profil vzniklý v průběhu výběrového řízení. Tyto údaje jsou zpracovávány do ukončení výběrového řízení, případně na delší dobu, na kterou uchazeč poskytl souhlas.

Zpracování údajů zaměstnanců jsou rozděleny na ty povinné na základě právní úpravy jako identifikační údaje, zdravotní pojišťovnu, vznik, případně zánik pracovního poměru, pracovní pozici, a jména dětí a manžela či manželky, kvůli daňovým účelům. Údaje, které správce zpracovává bez právní povinnosti jsou například telefon, email, kontaktní adresa, číslo bankovního účtu, nebo údaje o dosaženém vzdělání. Některé z údajů jsou poté předávány jiným subjektům jako je zdravotní pojišťovna zaměstnance, České správě sociálního zabezpečení, Finančnímu úřadu a Úřadu práce, pokud jde o cizince. Doba uchování údajů je odvozena příslušnými zákony, nejdelší záznamy se uchovávají pro účely důchodového pojištění, a to po dobu 30 let (Scio.cz, c 2021).

5.6 Malé podniky

V rámci kontaktování podniků s žádostí o zodpovězení mých dotazů na téma, jsem kontaktoval i některé mikro podniky. Jejich odpovědi se podobaly, byly stručné, ale vlastně přínosné. Jednalo se o podnik zemědělské výroby, druhý se zabýval deratizačními službami a prodejem deratizačních potřeb. V odpovědi stálo, že mají 5 a méně zaměstnanců, všechny údaje spravují sami, a personální otázky pro ně nejsou nijak zásadní. Monitoring neřeší pomocí technických zařízení, celý personál podniku je v denním kontaktu, a tak mají přehled o chodu firmy.

U první společnosti, obchodující s vejci, jsem na webových stránkách nenašel žádné osobní údaje. Kontakty jsou řešeny firemním emailem. Druhá společnost nabízí na webu telefonní čísla na konkrétní zaměstnance.

5.7 Vyhodnocení

Při vyhodnocování otázek na podniky bylo dokázáno, že jsou v těchto oblastech, konkrétně využívání zpracovatelů údajů, používání monitorování, zacházení s osobními údaji bývalých zaměstnanců a potenciálních zaměstnanců a školení o zacházení s osobními údaji, jsou pravidla benevolentní a podniky se v nich mohou chovat různě.

Dle vzorku podniků se dá usoudit, že tématu zabezpečení osobních údajů dávají více důrazu větší organizace, kde se zpracovává velké množství osobních údajů a pracuje s velkým množstvím subjektů údajů, tedy zaměstnanců. Z hlediska objemu dat se také dá předpokládat, že budou velké organizace lákavějším cílem pro napadení bezpečnosti osobních údajů. Na druhou stranu malé podniky ale musí být také na pozoru, protože by mohli být snazším cílem, kvůli nedostatečné znalosti problematiky.

V případě analyzovaných společností nebylo vypozorováno žádného rozporu s právními předpisy. Je důležité vzít v potaz, že k analýze podniků byli použity pouze údaje, které o sobě sami byli ochotni zveřejnit. Tím pádem by bylo překvapivé, kdyby se přiznali k vlastnímu zaváhání. I tak bylo nashromážděno množství zajímavých informací. Přínosnou může být zejména provedená analýza ohledně zveřejňování osobních údajů zaměstnanců na webových stránkách. Lze vypozorovat, že některé organizace si dokáží vystačit s minimem zveřejňovaných dat a jiné jich užívají více.

Nejčastěji dostupným osobním údajem zveřejňovaným na webových stránkách podniků bývají podle zkoumání autora webové adresy zaměstnanců, obsahující jejich jméno a příjmení. Úplně nejčastěji tak bývají zveřejněné osoby odpovědné za nábor nových zaměstnanců. Tento údaj se dá snadno nahradit adresou v obecném tvaru, bez udání jména kontaktní osoby, ale jen útvaru, který komunikaci obstarává. Řešení s příjmením ovšem zůstává osobitějším a budí větší důvěryhodnost podle mého názoru.

Autor oceňuje zveřejnění informací, týkající se zpracování osobních údajů zaměstnanců na webových stránkách, z důvodu, že se s nimi smí potenciální uchazeč o zaměstnání v dané společnosti seznámit, ještě před prvním nastoupením do výběrového řízení, a tedy před první vlnou zpracování osobních údajů.

ZÁVĚR

Cílem bakalářské práce bylo objasnit problematiku osobních údajů na úrovni podniků a otestování dostupnosti těchto dat ve vybraných společnostech.

V úvodu práce bylo vysvětleno, co to jsou osobní údaje a další základní pojmy, týkající se tématu, poté jsem se přesunul k procesu zpracování osobních údajů, kde bylo poukázáno na právní důvody zpracování, vysvětleny zásady zpracování a práva subjektů údajů a nastíněny důvody, proč je potřeba osobní údaje zabezpečovat. Po této kapitole následuje kapitola, kdy byl rozebrán na časové ose případ zaměstnance, jak z pohledu podniku přichází do kontaktu s osobními údaji ve třech fázích: před uzavřením pracovní smlouvy, během pracovního poměru a po jeho ukončení. Závěrečná kapitola byla věnována Monitoringu zaměstnanců za využití moderních technologií.

Praktická část obsahuje zkoumání dostupnosti osobních údajů na webových stránkách vybraných organizací a také zkoumání, jak ve stejných podnicích přistupují k některým problematikám tématu. Tento výzkum byl založen z části na přímém dotazování firem a z části z dostupných informacích na webových stránkách.

Dle názoru autora byl naplněn cíl práce. Bylo zanalyzováno pět organizací, zjištěny o nich zajímavé informace a porovnány s legislativou. Nebyla nalezena žádná odchylka, všechny zkoumané společností tedy podle autorova posouzení chrání osobní údaje zaměstnanců správně.

Autor dále věří, že práce nabídla přehledné shrnutí problematiky osobních údajů a může pro některé podniky sloužit jako jeden ze zdrojů informací, ze kterých mohou čerpat, a podle nichž mohou upravovat své vnitřní nastavení.

POUŽITÁ LITERATURA

BARTÍK, Václav a Eva JANEČKOVÁ, 2013. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 3. vyd. Praha: Linde Praha. Praktická právnická příručka. ISBN 978-80-86131-96-2.

BOZP info, 2018. *Můžeme se na pracovišti vzájemně informovat o platech?* [online]. BOZP info [cit. 2021-04-20]. Dostupné z: https://www.bozpinfo.cz/muzeme-se-na-pracovisti-vzajemne-informovat-o-platech

D'AMBROSOVÁ, Hana, 2002. *Ochrana osobních údajů při vedení personálních agend*. Praha: Pragoeduca. ESO (Pragoeduca). ISBN 80-731-0003-7.

Elegal.cz, 2019. *GDPR rok poté - na co se nejčastěji zapomíná?* [online]. Elegal.cz [cit. 2021-5-2]. Dostupné z: https://elegal.cz/gdpr-rok-pote-na-co-se-nejcasteji-zapomina

Eprávo, 2018. *Osoba zesnulá a GDPR* [online]. Eprávo [cit. 2021-03-31]. Dostupné z: https://www.epravo.cz/top/clanky/osoba-zesnula-a-gdpr-107890.html

Eprávo, 2019. *Zpracování biometrických údajů zaměstnanců* [online]. Eprávo [cit. 2021-03-31]. Dostupné z: https://www.epravo.cz/top/clanky/zpracovani-biometrickych-udaju-zamestnancu-109845.html

Eprávo, 2020. *Specifické aspekty ochrany osobních údajů 3/5* [online]. Eprávo [cit. 2021-03-31]. Dostupné z: https://www.epravo.cz/top/clanky/serial-specificke-aspekty-ochrany-osobnich-udaju-35-anonymizace-a-pseudonymizace-v-ochrane-dat-a-informaci-111200.html

Eprávo.cz [online], 2018. Eprávo.cz [cit. 2021-5-7]. Dostupné z: https://www.epravo.cz/top/clanky/vybrane-aspekty-socialni-site-linkedin-ve-svetle-gdpr-107540.html?mail

Eprávo.cz, 2020. *Může si zaměstnavatel přečíst e-maily bývalého zaměstnance?* [online]. Eprávo.cz [cit. 2021-5-5]. Dostupné z: https://www.epravo.cz/top/clanky/muze-si-zamestnavatel-precist-e-maily-byvaleho-zamestnance-111482.html

Evropská komise, -. *Kdo je to správce údajů nebo zpracovatel údajů?* [online]. Evropská komise [cit. 2021-03-31]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_cs

Evropská komise, c 2004. *Co jsou to osobní údaje?* [online]. Evropská komise [cit. 2021-03-31]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs

GDPR.cz, -. *Zpracování osobních údajů* [online]. GDPR.cz [cit. 2021-04-02]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zpracovani-osobnich-udaju/

GDPR.cz, 2018. *Jak poznám, jestli jsem správcem nebo zpracovatelem osobních údajů?* [online]. GDPR.cz [cit. 2021-03-31]. Dostupné z: https://www.gdpr.cz/blog/spravcem-nebo-zpracovatelem/

Chrarvát group s.r.o. [online], C 2021. [cit. 2021-5-26]. Dostupné z: https://www.charvat-chs.cz

JANEČKOVÁ, Eva, 2018. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer. ISBN 978-80-7552-248-1.

JOUZA, Ladislav, 2018. Ústav práva a právní vědy. *Osobní spis zaměstnance - ano či ne* [online]. Ústav práva a právní vědy [cit. 2021-04-19]. Dostupné z: https://www.ustavprava.cz/blog/2018/09/osobni-spis-zamestnance-ano-ci-ne/

Komerční banka [online], C 2021. [cit. 2021-5-27]. Dostupné z: https://www.kb.cz/cs/

KUČEROVÁ, Dagmar, 2018. Podnikatel.cz. *GDPR a výmaz osobních údajů po skončení pracovního poměru* [online]. Podnikatel.cz [cit. 2021-04-23]. Dostupné z: https://www.podnikatel.cz/clanky/gdpr-a-vymaz-osobnich-udaju-po-skonceni-pracovniho-pomeru/

Man.eu, c 2021. *Kariéra* [online]. [cit. 2021-6-1]. Dostupné z: https://www.man.eu/cz/cz/o-nas/kariera-u_spolecnosti-man/kariera-u_spolecnosti-man.html

Manoriginal.cz, c 2021. *Zaměstnání v MAN* [online]. [cit. 2021-6-1]. Dostupné z: https://www.manoriginal.cz/zamestnani-v-man/

MIHULOVÁ, Jitka a Martin KORNEL, 2018. Frank Bold Advokáti. *Co je, co není, a co bude osobní údaj podle GDPR* [online]. [cit. 2021-03-31]. Dostupné z: https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdp

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

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

NEZMAR, Luděk, 2017. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing. Právo pro praxi. ISBN 978-80-271-0668-4.

Parkon.cz [online], C 2021. [cit. 2021-6-21]. Dostupné z: https://www.parkon.cz

PAVLOVIČOVÁ, Jana, 2017. 22 Hlav. *Definice osobních údajů podle GDPR* [online]. [cit. 2021-03-31]. Dostupné z: https://www.bvmaudit.cz/definice-osobnich-udaju-podle-gdpr

Podnikatel.cz, 2019. *Zpracování fotografií zaměstnanců vyžaduje opatrnost. Na co si dát pozor?* [online]. Podnikatel.cz [cit. 2021-5-7]. Dostupné z: https://www.podnikatel.cz/clanky/zpracovani-fotografii-zamestnancu-vyzaduje-opatrnost-na-co-si-dat-pozor/

Práce a mzda, 2017. *Ochrana osobních údajů zaměstnanců od A (přes GDPR) do Z* [online]. Práce a mzda [cit. 2021-04-15]. Dostupné z: https://www.praceamzda.cz/clanky/ochrana-osobnich-udaju-zamestnancu-od-pres-gdpr-do-z

Právní prostor, 2019. *Monitoring zaměstnanců: Práva a povinnosti zaměstnavatelů při zpracování osobních údajů* [online]. Právní prostor [cit. 2021-5-2]. Dostupné z: https://www.pravniprostor.cz/clanky/pracovni-pravo/monitoring-zamestnancu-prava-a-povinnosti-zamestnavatelu-pri-zpracovani-osobnich-udaju

Scio.cz [online], c 2021. [cit. 2021-6-7]. Dostupné z: https://www.scio.cz/nsz/?gclid=Cj0KCQjwh_eFBhDZARIsALHjIKeYtfA12oCqOoLJZAGu6N-DnwYpVffmUg3sxP-IHc-0I6qLkCAGcewaAgrIEALw_wcB

Scio.cz, c 2021. *Informace o zpracování osobních údajů zaměstnanců a uchazečů o zaměstnání* [online]. [cit. 2021-6-7]. Dostupné z: https://www.scio.cz/osobni-udaje/udaje-zamestnanci.asp

Úřad pro ochranu osobních údajů, 2017. *Zvláštní kategorie osobních údajů* [online]. Úřad pro ochranu osobních údajů [cit. 2021-03-31]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaju-citlive-udaje/d-27274/p1=4744

Úřad pro ochranu osobních údajů, 2019. *Zásady a právní důvody zpracování* [online]. Úřad pro ochranu osobních údajů [cit. 2021-04-03]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

Úřad pro ochranu osobních údajů, c 2013. *Slovníček nejdůležitějších pojmů* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2021-03-31]. Dostupné z: https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617

Zákon č. 435/2004 Sb., Zákon o zaměstnanosti, In: *Sbírka zákonů České republiky*, 1.října 2004, ISSN 1211-1244.