MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC
Ústav informatiky a aplikované matematiky

Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů

BAKALÁŘSKÁ PRÁCE

Vítězslava Nováková
Vedoucí práce: Ing. Lukáš Pavlík

Olomouc 2019

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci na téma „Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů“ vypracovala samostatně a použila jen zdroje v seznamu literatury a použitých zdrojů.

Tištěná verze textu práce je shodná s textem práce na CD nosiči a elektronickou verzí vloženou do studijního systému IS/STAG.

Ve Šternberku dne 19. 6. 2019

Vítězslava Nováková

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala vedoucímu mé bakalářské práce, Ing. Lukáši Pavlíkovi, za ochotu při konzultacích, cenné rady, podnětné připomínky a trpělivost v průběhu zpracování práce.

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vítězslava Nováková**
Osobní číslo:	**M16043**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Název tématu:	**Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů**
Téma anglicky:	**The Issue of GDPR and its Impact on Employers in the Field of Personal Data Protection**
Zadávající katedra:	**Ústav informatiky a aplikované matematiky**

Zásady pro vypracování:

Popište základní problematiku legislativy GDPR.
Charakterizujte vybranou organizaci.
Proveďte komplexní analýzu vybrané organizace s důrazem na zavedení směrnice GDPR.
Vyhodnoďte výsledky provedné anylýzy a navrhněte vlastní způsob řešení.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

ŽÚREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017. Právo. ISBN 978-80-7554-097-3.
NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
VOIGT, PAUL & VON DEM BUSSCHE, AXEL: The Eu General Data Protection Regulation: A Practical Guide. SPRINGER 2017. ISBN: 9783319579580.
NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 (tzv. GDPR).
KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech. Praha: Bova Polygon, 2013, 168 s. ISBN 978-80-7273-173-2.
ZÁKON č. 101/2000 Sb., O OCHRANĚ OSOBNÍH ÚDAJŮ.

Vedoucí bakalářské práce: **Ing. Lukáš PAVLÍK**
Ústav informatiky a aplikované matematiky

Datum zadání bakalářské práce: **25. května 2018**
Termín odevzdání bakalářské práce: **29. března 2019**

Podpis studenta: ..... Datum: 13. 9. 2018

Podpis vedoucího práce: ..... Datum: 13. 6. 2018

Mgr. Irena KOVAČIČLNOVÁ
prorektorka

L.S.

PhDr. Mgr. Zdeňka KRIŠOVÁ, Ph.D.
manažer ústavu

V Olomouci dne 4. června 2018

Obsah

Úvod

V dubnu 2016 došlo k přijetí Obecné nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679 neboli General Data Protection Regulation (nadále v práci označováno jako „GDPR“ popř. „Nařízení“),[1] česky označováno jako Obecné nařízení o ochraně osobních údajů, s účinností 25. 5. 2018.[2] Od tohoto data je aplikovatelné na celém území Evropské unie, tedy i v České republice, a všechny subjekty zpracovávající osobní údaje fyzických osob jsou povinny se jím řídit. EU tímto dokončila komplexní reformu oblasti ochrany osobních údajů v Evropě. „*Reforma stojí na několika pilířích (stěžejních složkách): jednotná pravidla, zjednodušené postupy, koordinované akce, zapojení uživatelů, efektivnější informace a větší vymáhací pravomoci*.“[3]

Nařízení přináší změny v oblasti ochrany osobních údajů a společnostem, které disponují osobními údaji, ukládá nemálo nových povinností. Změny v oblasti ochrany osobních údajů se týkají taktéž zaměstnavatelů, když tito disponují osobními údaji svých zaměstnanců a nadále s nimi pracují. Tato práce se bude zabývat především konkrétními dopady daného nařízení na zaměstnavatele, budou zde popsány kroky, které budou zaměstnavatelé nuceni podniknout pro to, aby nařízení plně vyhověli, a dále budou zmíněny možné sankce za nedodržení nařízení. Součástí práce budou taktéž doporučení pro zaměstnavatele, jak splnit veškeré požadavky nařízení.

Cílem této bakalářské práce je popsat rozdíly v povinnostech zaměstnavatelů v období před zavedením nařízení GDPR a po jeho účinnosti, důraz bude kladen především na povinnosti nově vyplývající z nařízení. Práce je rozdělena na teoretickou a praktickou část. Teoretická část obsahuje obecné informace o GDPR, jeho působnosti a hlavní znaky. V rámci praktické části práce bude proveden průzkum v organizaci Gymnázium Šternberk ohledně praktických dopadů implementace Nařízení a následně finální částí práce bude vyhodnocení výsledků dotazníkového šetření a návrh doporučení.

---

[1] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, strana 16.
[2] KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018, strana 10.
[3] *Evropský sbor pro ochranu osobních údajů: Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679* 17 [online]. [cit.3.4.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886.

Teoretická část

1 Co je GDPR

Zkratkou GDPR rozumíme Obecné nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Předmětná zkratka pochází z anglického názvu nařízení, tedy General Data Protection Regulation. GDPR je (jakožto i každé jiné nařízení EU) právně závazné v celém svém rozsahu a přímo účinné ve všech členských zemích Evropské unie. Tímto je myšleno, že má stejnou závaznost jako zákony přijaté Parlamentem České republiky, a to aniž by bylo třeba jej začlenit do stávajících zákonů, popřípadě přijmout zákon nový. Mimo státy EU je nařízení závazné taktéž pro některé další země, a to Lichtenštejnsko, Norsko a Island.[4]

Cílem Nařízení je „*přispět k dotvoření prostoru svobody, bezpečnosti a práva a hospodářské unie, k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobrým životním podmínkám fyzických osob*.“[5]

Nařízení však není první právní úpravou k ochraně osobních údajů fyzických osob zavedenou EU, tímto byla již Směrnice ES 95/46/ES z roku 1995. Směrnice však na rozdíl od nařízení nejsou pro členské státy závazné v celém svém rozsahu a přímo účinné, pouze země zavazují k dosažení deklarovaného cíle.[6] Tento si však každý stát může vyložit po svém, stejně tak není sjednocen způsob, jak daného cíle dosáhnout, tento je taktéž ponechán na libovůli jednotlivých členských zemích. K přijetí nového nařízení bylo proto přistoupeno s ohledem na zaostalost původní směrnice. Ta nejenže nebyla schopna zajistit sjednocení právní úpravy ochrany osobních údajů na celém území EU, jelikož tato se v jednotlivých zemích poměrně výrazně lišila a tento fakt následně způsoboval problémy zpracovatelům údajů působícím ve vícero zemích EU,[7] postupem času však původní směrnice také přestala

[4]KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018, strana 9

[5]NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Úř. věst. L 119 4.5.2016, strana 1.

[6] Šandera, David: *Dopady obecného nařízení o ochraně osobních údajů na firemní procesy.* Diplomová práce, VŠT v Praze, 2017. Strana 13.

[7]*Ministerstvo vnitra České republiky. Orientace v GDPR* [online]. [cit. 3. 4. 2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx.

odpovídat současné rychle se měnící době, především co se týče prostředků, které jsou ke zpracovávání osobních údajů využívány. Oproti předchozí v tomto směru nejednoznačné Směrnici nově vydané Nařízení také specifikovalo svou územní působnost. GDPR přímo stanoví, že je aplikovatelné na všechny organizace, které zpracovávají osobní údaje subjektů sídlících na území Evropské unie, a to bez ohledu na lokaci jejich vlastního sídla. Nařízení se tedy vztahuje také na organizace sídlící mimo EU, které zpracovávají osobní údaje zde rezidujících subjektů.[8]

Nařízení na původně platnou směrnici z velké části navazuje, nejedná se o stoprocentně nově vytvořenou úpravu. Základní body předchozí směrnice byly přejaty a dále rozpracovány a následně doplněny o nové části.

Nejdůležitější podobnosti a rozdíly:[9]

HLAVNÍ ROZDÍLY	PŘEJATÉ OBLASTI
posílení působnosti (více oblastí práva EU, dopad i na správce mimo EU)	většina hlavních definic
posílení ochrany dětí	většina zásad a principů ochrany údajů
více požadavků na správce a zpracovatele	většina práv subjektů
sjednocení a zvýšení sankcí	většina povinností správců údajů
nová práva subjektů údajů (právo být zapomenut, právo na přenositelnost osobních údajů)	zásadní prvky postavení nezávislých dozorových úřadů
funkce pověřence pro ochranu osobních údajů	koncept výjimek pro privilegovaná zpracování (archivní, vědecká, historická apod.)
sjednocení pravomocí dozorových úřadů	koncept výjimek pro ochranu veřejných zájmů (bezpečnost, ekonomika apod.)

Tabulka 1: Porovnání Obecného nařízení a Směrnice 95/46 ES

[8] Šandera, David: *Dopady obecného nařízení o ochraně osobních údajů na firemní procesy.* Diplomová práce, VŠT v Praze, 2017. Strana 16.

[9] Přejato z Důvodové zprávy k Zákonu č. 110/2019, Sb. o zpracování osobních údajů. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0.

Již před zavedením GDPR měly subjekty zpracovávající osobní údaje určité povinnosti, jak s těmito nakládat (v českém prostředí se řídily již výše zmíněným zákonem o ochraně osobních údajů). Dříve platné zásady a pojmy tedy nadále platí a nedošlo k jejich změně.

Pro menší zpracovatele osobních údajů nepřináší Nařízení nijak velkou revoluci v přístupu k nim, naopak větší správci osobních údajů (např. telekomunikační společnosti, banky, velcí zaměstnavatelé) se musejí připravit na vyšší nároky, jež na ně budou v souvislosti s uchováváním a zpracováváním osobních údajů kladeny.[10]

Obecným nařízením je od května 2018 povinen řídit se každý subjekt, který provádí zpracování osobních údajů, takový subjekt je nazýván správcem osobních údajů. Řídit se jím musí také všechny subjekty, které osobní údaje dále zpracovávají, tedy tzv. zpracovatel. Práva z nařízení pak naopak vyplývají fyzickým osobám – subjektům údajů. Obecným nařízením jsou povinni se řídit také dozorové úřady, v ČR se jedná o Úřad pro ochranu osobních údajů.[11]

2 Zákon o zpracování osobních údajů

Původní směrnici 95/46/ES na území České republiky implementoval zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů,[12] tento byl od 25. května 2018 nahrazen Nařízením. Zákon o ochraně osobních údajů se ruší účinností změnového neboli adaptačního zákona, který reflektuje nové požadavky na ochranu osobních údajů zavedené právě GDPR na území ČR.[13]

Adaptační zákon se však Česku (jako jedné z mála zemí) do účinnosti nařízení nepodařilo připravit a schválen byl poslanci až s několikaměsíčním zpožděním v prosinci 2018.[14] V lednu 2019 nicméně došlo k dalšímu prodlení, o které se zasadil Senát České republiky, který navrhl v zákoně několik změn a normu bylo proto třeba Sněmovnou spolu s pozměňovacími návrhy znovu projednat.[15] Dne 12. 3. 2019 pak došlo konečně ke schválení

[10] *Úřad pro ochranu osobních údajů: Základní příručka k GDPR* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2075.
[11] *Tamtéž.*
[12] KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018, strana 9.
[13] *Úřad pro ochranu osobních údajů: Základní příručka k GDPR* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2075.
[14] *GDPR.cz: Adaptační zákon prošel sněmovnou* [online]. Změněno 2. 1. 2019. Dostupné z: https://www.gdpr.cz/blog/adaptacni-zakon-prosel-snemovnou/.
[15] *Podnikatel.cz. Další zpoždění, Senát adaptační zákon k GDPR vrátil. Víme, co nového přináší* [online].

zákona, a to ve znění, v jakém byl Senátem poslancům vrácen. Konečně tedy došlo k implementaci Nařízení do českého vnitrostátního práva a zákon č. 110/2019 Sb., o zpracování osobních údajů (také označován jako adaptační zákon) nabyl účinnosti svým vyhlášením ve sbírce zákonů dne 24. 4. 2019. Od tohoto dne tak má Česká republika nová platná pravidla pro oblast ochrany soukromí.[16] Tímto byl zároveň zrušen dosud účinný Zákon č. 101/2000 Sb., o ochraně osobních údajů.[17]

Adaptačním zákonem došlo k upřesnění a rozvedení Nařízení, když toto dovoluje jednotlivým členským zemím „*odchýlit se od obecné úpravy a přijmout určité národní výjimky, které jsou lépe uzpůsobeny konkrétnímu právnímu prostředí*.“[18]

U některých ustanovení tedy Nařízení umožňuje (a také předpokládá) další zpřesnění v rámci národní legislativy. Na příklad došlo ke snížení horní hranice správních pokut pro případ neplnění některé z povinností nebo porušení některého ze zákazů v oblasti ochrany osobních údajů, které lze za jednotlivá porušení právních předpisů uložit. ÚOOÚ pak může od uložení pokuty zcela upustit v případě, že se takového přestupku dopustí orgány veřejné moci. Maximální výší je 1 000 000 Kč, popřípadě 5 000 000 Kč, a to v případech, kdy se jedná o přestupek spáchaný prostřednictvím tisku, filmu, rozhlasu, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.[19]

Dále jsou v Zákoně jasně vymezeny pravomoci a postavení Úřadu pro ochranu osobních údajů, do jehož kompetence nyní spadá řešení sporů v oblasti práva na informace, provádění opatření k odstranění nedostatků při zjištění porušení povinností vyplývajících z Nařízení a stanovení přiměřené lhůty pro jejich odstranění a dále udělování sankcí v případech, kdy k odstranění nedostatků není přistoupeno.[20]

Přijetí adaptačního zákona však v praxi pravděpodobně nebude mít nijak dalekosáhlé dopady, jelikož tento pouze zpřesňuje práva a povinnosti již dříve stanovená Nařízením.

Změněno dne 1. 2. 2019. Dostupné z: https://www.podnik/atel.cz/clanky/adaptacni-zakon-k-gdpr-upresnuje-pokuty-a-vekove-omezeni-pro-udeleni-souhlasu/.

[16] *Uoou.cz: Adaptační legislativa k GDPR vstoupila v účinnost* [online]. Změněno dne 25. 4. 2019. Dostupné z: https://www.uoou.cz/adaptacni-legislativa-k-nbsp-gdpr-vstoupila-v-nbsp-ucinnost/d-33656.

[17] *Epravo.cz: Nový zákon o zpracování osobních údajů* [online]. Změněno dne 30. 5. 2019. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html.

[18] Tamtéž.

[19] § 61 odst. 2 Zákona č. 110/2019, Sb., o zpracování osobních údajů.

[20] § 2e) Zákona č. 110/2019, Sb., o zpracování osobních údajů.

3 Definice základních pojmů

Mezi nejdůležitější pojmy, jež budou v této práci používány, lze zařadit následující:

- osobní údaj,
- citlivý osobní údaj,
- subjekt údajů,
- zpracování osobních údajů,
- zpracovatel osobních údajů,
- správce osobních údajů,
- pověřenec pro ochranu osobních údajů.

3.1 Osobní údaj

Základním pojmem, se kterým nová právní úprava pracuje, je osobní údaj. Jeho význam je (stejně jako i veškeré další pojmy v Nařízení použité) vymezen ve článku 4 Nařízení, konkrétně hned v prvním odstavci, a to tak, že se jím rozumí „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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*.“[21] Definice je tedy stanovena poměrně široce, aby pod ni bylo možno zařadit co největší množství informací, které je třeba Nařízením chránit. Pod pojem osobní údaje tedy nespadají pouze očividné informace jako je jméno a příjmení dané osoby, její rodné číslo, adresa apod., ale například také celý obsah personálního spisu zaměstnance, tedy také jeho pracovní hodnocení, docházkový list nebo fotografie, v rámci transakčních vztahů se pak může jednat o historii objednávek zákazníka a historie jím prováděných plateb.[22] Jedná se tedy o pojem zahrnující poměrně širokou škálu informací týkajících se dané osoby.

[21] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 4.

[22] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 6.

3.2 Citlivý osobní údaj

Speciální podkategorií osobních údajů jsou tzv. citlivé osobní údaje, které se řídí speciálním režimem. Jedná se o údaje vymezené ve druhé části odst. 1 čl. 4 Nařízení, tedy údaje odhalující rasový či etnický původ osoby, její náboženské vyznání, politický názor, dále sem spadá veškerý genetický materiál osoby (vzorky DNA), biometrické údaje (otisky prstů), údaje o sexuální orientaci nebo o zdravotním stavu a osobní údaje dětí.[23] Tyto údaje, které fyzické osoby běžně považují za výjimečně citlivé právě s ohledem na jejich intimní povahu, je zpracovatel povinen obzvláště chránit a při jejich zpracování jsou na něj kladeny vyšší požadavky.

3.3 Subjekt údajů

Subjektem údajů je fyzická osoba, které se osobní údaje týkají.[24] Nikdy nemůže jít o osobu právnickou, informace týkající se právnických osob tedy nejsou osobními údaji. Subjekty mohou být pouze žijící fyzické osoby, když na již zesnulé se Nařízení nevztahuje. Subjekty jsou tedy obyvatelé Evropské unie, kteří jsou Nařízením chráněni.

3.4 Zpracování osobních údajů

Zpracováním osobních údajů je myšlena „jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“[25] Jak je z definice vidno, zpracováním není jen nakládání s osobními údaji (tedy aktivní činnost), ale také jejich uchovávání (pasivní činnost), popř. dokonce jejich likvidace.

---

[23] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 6.

[24] *Úřad pro ochranu osobních údajů: Základní příručka k GDPR* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293

[25] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 4.

3.5 Zpracovatel osobních údajů

Zpracovatelem je pak osoba s údaji disponující, jedná se o „fyzickou nebo právnickou osobu, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce,“[26]pro účely této práce se jím bude rozumět především zaměstnavatel nakládající s osobními údaji svých zaměstnanců.

3.6 Správce osobních údajů

Správce se od zpracovatele liší v tom, že se jedná o „subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.“[27] Správce dává zpracovateli pokyny, jakým způsobem a z jakého důvodu má s údaji nakládat, a to pro konkrétní účel. Zpracovatel tedy jedná pouze na základě předchozích pokynů správce.

V některých případech však mohou tyto funkce splývat, subjekt může být jak správcem údajů, tak i jejich zpracovatelem. Přesně o takovouto situaci se jedná v případě zaměstnavatele. Ten shromažďuje údaje o svých zaměstnancích, které následně zpracovává. Zaměstnanci v případě pracovněprávních vztahů nikdy nejsou zpracovateli, jsou pouze správci svých osobních údajů.

3.7 Pověřenec pro ochranu osobních údajů

Zcela novým pojmem zavedeným Nařízením je pověřenec pro ochranu osobních údajů. Správce (případně zpracovatel) do této funkce ustanoví osobu, jejímž úkolem je „*nezávislý dohled nad dodržováním povinností v oblasti ochrany osobních údajů*.“[28]

Jedná se buď o jednoho ze zaměstnanců, který je pro tuto funkci speciálně vyškolen, případně je možné, aby ji vykonával externista na základě smlouvy se zaměstnavatelem.

Zřízení této funkce není povinné pro všechny subjekty, tento závazek mají především orgány veřejné moci a subjekty provádějící rozsáhlé shromažďování údajů.[29] Provádí-li tedy

[26] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 4.

[27] Tamtéž.

[28] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 8.

[29] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně

zaměstnavatel pouze zpracování údajů v běžném rozsahu nutné pro plnění jeho povinností, funkci pověřence zřizovat nemusí. Nic mu však nebrání v tom, aby tuto funkci zřídil dobrovolně.

4 Základní zásady

V článku 5 Nařízení jsou specifikovány zásady zpracování osobních údajů, na kterých je Nařízení postaveno a ze kterých následně vycházejí konkrétní povinnosti správce a zpracovatele. Stručně je lze shrnout následujícím způsobem:

- zákonnost, korektnost, transparentnost,
- omezení účelu,
- minimalizace údajů,
- přesnost,
- omezení uložení,
- integrita a důvěrnost,
- odpovědnost.

Dle shora uvedených zásad je od správce a zpracovatele vyžadováno, aby byly osobní údaje zpracovávány na základě určitého právního důvodu a v souladu se zákonem a pouze ve stanoveném rozsahu a jen pro nezbytnou dobu. Zpracování osobních údajů je tedy primárně zakázáno, ledaže je k němu dán zákonný důvod.[30] Vůči subjektu údajů musí jít o transparentní zpracování, tedy musí být zajištěna co nejvyšší míra informovanosti subjektů a tom, jak bylo s údaji naloženo, tyto informace musí být snadno přístupné a podávané za použití jednoduchých a jasných jazykových prostředků.[31] Subjekty musí být informovány o tom, proč jsou jejich údaje shromažďovány, jak dlouho budou uchovány a kdo konkrétně k nim má přístup. Osobní údaje nesmí být zpracovány za jiným účelem, než k jakému byly primárně shromážděny, organizace nejsou oprávněny shromažďovat náhodné informace, aniž by tak

---

fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 37 odst. 1.

[30] Voigt, Paul & von dem Bussche, Axel. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Strana 5.

[31] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Bod 39 odůvodnění.

činily za předem definovaným účelem, údaje pak musí být shromažďovány pouze v takovém rozsahu, který je pro zajištění stanoveného účelu nezbytný, údaje musí být přesné a dle potřeby pravidelně aktualizované. V případě, že údaje již nejsou zapotřebí, nepotřebné údaje budou vymazány, případně anonymizovány, za účelem zajištění integrity a důvěrnosti budou přijata vhodná technická a organizační opatření, jak dosáhnout standardu která zajistí, že data nemohou být zneužita třetí osobou či že budou ztracena. V neposlední řadě je třeba, aby správce i zpracovatel zajistil, že s osobními údaji bude nakládáno dle předmětných zásad a v případě potřeby bude schopen prokázat, že tomu tak skutečně bylo.[32]

5 Povinnosti zaměstnavatele při zpracování osobních údajů zaměstnanců

Každý zaměstnavatel disponuje poměrně širokou škálou osobních údajů týkajících se všech jeho zaměstnanců. Tyto začne sbírat dokonce ještě před uzavřením pracovněprávního vztahu, především ve formě životopisů či motivačních dopisů, které mu zasílají zájemci o zaměstnání, kde tito o sobě prozrazují informace, jako jsou jejich příjmení, jméno, datum narození, adresa, státní občanství, studijní a pracovní historie, dovednosti a zájmy, součástí těchto dokumentů pak často bývá také jejich fotografie. Ve sbírání informací následně zaměstnavatel pokračuje uzavřením pracovní smlouvy, která vždy musí obsahovat již shora uvedené identifikační údaje zaměstnance. Zaměstnavatel se posléze často dozví o rodinných poměrech svého zaměstnance (například pobírá-li tento na své děti slevu na dani, zaměstnanec musí dodat také jejich údaje, tedy jméno, příjmení a rodné číslo, pro účely daňového přiznání jsou důležité údaje také o manželovi/manželce, registrovaném partnerovi).

Za účelem výpočtu mzdy či platu je pro zaměstnavatele často nutno mít informace o předchozí praxi zaměstnance (pro zařazení do správné platové třídy a platového stupně apod.) a pro její následné vyplácení číslo jeho bankovního účtu, za účelem provádění plateb na zdravotní pojištění je nutno znát zdravotní pojišťovnu zaměstnance. Zaměstnavatel se dozví taktéž o zdravotních znevýhodněních zaměstnance (nutno pro plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců) případně o těhotenství zaměstnankyň.

[32] *Evropská komise: Zásady GDPR* [online]. [cit. 3. 4. 2019]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_cs.

V průběhu trvání pracovního poměru shromažďování údajů samozřejmě pokračuje. Na zaměstnance jsou psána jeho nadřízenými pracovní hodnocení, která jsou taktéž osobním údajem, stejně jako informace o jeho docházce či mzdové listy. V případě, že je zaměstnanec v rámci pracovního výkonu monitorován (například bezpečnostními kamerami nebo nahráváním telefonických hovorů), i v takovémto případě se jedná o zpracovávání osobních údajů zaměstnanců.

Z uvedeného (a pouze demonstrativního, nikoli taxativního) výčtu je tedy evidentní, že zaměstnavatel s postupujícím časem o zaměstnanci nashromáždí opravdu velké množství různých informací. Veškeré tyto údaje nadále zůstávají vlastnictvím zaměstnanců, ti je zaměstnavateli pouze propůjčují k dalšímu zpracování za konkrétním (předem dohodnutým) účelem.[33]

Ze zásady integrity a důvěrnosti vyplývá pro zaměstnavatele povinnost zajistit technická a organizační opatření, která zajistí bezpečnost osobních údajů jeho zaměstnanců. Jejich účelem tedy je zabránit neautorizovanému zveřejnění údajů, manipulaci s nimi či dokonce zajisti, že nedojde k jejich zničení. Z praktického hlediska lze daná opatření rozdělit do třech základních kategorií:

- opatření fyzické bezpečnosti,
- opatření informační bezpečnosti,
- opatření personální bezpečnosti.[34]

5.1 Fyzická bezpečnost

Fyzickou bezpečností je myšleno zajištění prostor, kde jsou osobní údaje zaměstnanců umístěny, popř. zabezpečení nosičů, na nichž jsou skladovány. Tato opatření se týkají především zajištění materiální bezpečnosti prostor. Příkladem může být, že kartotéková skříň, kde se nachází personální složky zaměstnanců, bude zajištěna funkčním zámkem, klíč k ní bude svěřen pouze prověřené osobě a skříň sama bude uložena na místě, kam nemají přístup cizí osoby, případně zajištění kamerového systému, jež bude prostory dodatečně chránit.

[33] *Úřad pro ochranu osobních údajů: Zaměstnavatel jako správce osobních údajů* [online]. Změněno 13. 12. 2013. Dostupné z: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171/p1=3938.

[34] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 16.

5.2 Informační bezpečnost

Informační bezpečností je míněno softwarové zabezpečení a ochrana elektronicky vedených údajů. Tímto je myšleno především posílení bezpečnosti informačních systémů a ochrana kybernetické bezpečnosti. Součástí těchto opatření může být také řádné proškolení všech zaměstnanců, jak nakládat se svěřenou výpočetní technikou, tak, aby nedošlo k narušení její bezpečnosti.

5.3 Personální bezpečnost

Pod pojmem personální bezpečnost je pak možno podřadit stanovení postupů při nakládání s osobními údaji, omezení přístupových oprávnění pouze na autorizované osoby a taktéž omezení rozsahu, ve kterém mají tyto osoby k údajům přístup pouze na informace nutně nezbytné k výkonu jejich práce.

5.4 Opatření

Konkrétní opatření je nutno zvolit s ohledem na konkrétní rizika, která s předmětným zpracováním osobních údajů souvisejí. Stejně tak je třeba, aby byla přiměřená rozsahu a účelu zpracování. Samozřejmě je třeba zohlednit také ekonomické možnosti daného zaměstnavatele, volba vhodných technologických a personálních opatření je ve velké míře závislá právě od jeho finančních možností. Těžko lze od zaměstnavatele o několika málo zaměstnancích očekávat stejnou míru zabezpečení jeho prostor a systémů jako od organizací zaměstnávající stovky osob a působících na několika různých pracovištích. Každý zaměstnavatel by tedy měl především usilovat o *„snížení rizika na úroveň, která je statisticky akceptovatelná*.“[35] Menší zaměstnavatelé tedy pravděpodobně přijmou poměrně jednoduchá opatření, zahrnující určené prostory pro uchovávání informací (jako již výše zmíněná kartotéková skříň), které je možné zamknout a předání klíčů pouze několika pověřeným osobám spolu se zajištěním kybernetické bezpečnosti prostřednictvím dalšího zaměstnance. Větší společnosti pak často přistoupí ke komplexnější bezpečnostní politice sestávající z mnoha různých oddělení zajišťujících různé úkoly (IT tým, právní oddělení, bezpečnostní agentura, oddělení lidských

[35] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 15.

zdrojů apod.).

6 Práva zaměstnanců

Nařízení přiznává subjektům různá práva. Oproti původní právní úpravě jsou práva subjektů Nařízením posílena, některá nová práva byla dokonce zavedena. Jedná se například o právo na přenositelnost, které se v dosavadní české právní úpravě před zavedením GDPR nevyskytovalo. [36]

6.1 Základní práva zaměstnanců

Základním právem všech zaměstnanců je být informován o tom, že zaměstnavatel jeho osobní informace vůbec zpracovává či teprve zpracovávat v budoucnu hodlá. Tato informace zpravidla bývá ze strany zaměstnavatele zaměstnanci poskytnuta hned při prvním styku stran, tedy bývá již součástí nabídky práce. Ta obsahuje upozornění, že podáním přihlášky potenciální zaměstnanec souhlasí se zpracováním svých osobních údajů a také informaci, jak bude s poskytnutými osobní údaji naloženo po skončení výběrového řízení (v případě neúspěšných kandidátů dochází k jejich skartaci, u těch úspěšných pak započetím pracovněprávního vztahu naopak dochází ze strany zaměstnavatele ke sběru dodatečných osobních údajů). Souhlas bývá udělen za konkrétním účelem, tento tedy musí být zaměstnanci předem znám. Tato tzv. informační povinnost je založena článkem 13 Nařízení.

Zaměstnanec má dále právo na informaci, za jakým účelem budou jeho osobní údaje zpracovávány, kdo je správcem těchto údajů (tedy totožnost zaměstnavatele) a kdo je příjemcem údajů. Mezi další práva pak patří:

- právo na přístup k osobním údajům,
- právo na opravu těchto údajů,
- právo na jejich výmaz,
- právo na jejich přenositelnost,
- právo na omezení zpracování,
- právo vznést námitku proti zpracování údajů, kdy správce musí prokázat, že má pro jejich zpracování oprávněné závažné důvody.[37]

[36] *GDPR.cz: Přenositelnost* [online]. Změněno 31. 1. 2018. Dostupné z: https://www.gdpr.cz/blog/prenositelnost/.

[37] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně

Zaměstnanec má právo na získání svých osobních údajů. Spolu s nimi má právo na poskytnutí údajů o tom, za jakým účelem jsou jeho údaje zpracovávány, kdo je jejich příjemcem a po jak dlouhou dobu budou údaje u zpracovatele uloženy. V případech, kdy jsou osobní údaje nesprávné či neúplné, má zaměstnanec právo požadovat jejich opravu či doplnění, kdy zaměstnavatel je povinen po předchozím upozornění ze strany zaměstnance tuto opravu provést. Právo na výmaz či také právo být zapomenut pak představuje povinnost zaměstnavatele zlikvidovat osobní údaje, pokud tyto již nejsou potřebné pro účel, za kterým byly shromážděny, případně pokud zaměstnanec o jejich výmaz požádá a zároveň neexistuje žádný právní důvod, proč by zaměstnavatel údaje potřeboval k další činnosti. K výmazu je třeba přistoupit také za situace, kdy osobní údaje byly zpracovány protiprávně. Právo na přenositelnost údajů je zcela novým právem zavedeným Nařízením. Jeho podstatou je možnost získat osobní údaje, které se subjektu údajů týkají a který je správci dříve poskytl, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a následně právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Takovéto zpracování musí být možno provést automatizovaně, tedy musí být technicky proveditelné.[38]

6.2 Princip proporcionality

Jak je výše uvedeno, zaměstnanec má právo na přístup k zaměstnavatelem zpracovávaným údajům. Veškeré tyto údaje zaměstnavatel poskytuje zaměstnanci bezplatně. Nicméně tohoto práva nesmí zaměstnanec zneužívat. V případech, kdy je žádost zaměstnance zjevně nedůvodná či nepřiměřená (na příklad z důvodu častých opakování takovýchto žádostí), může zaměstnavatel buď odmítnout žádosti vyhovět, případně stanovit poplatek zohledňující související administrativní náklady, za jehož úhradu bude žádosti vyhověno. Zjevnou nedůvodnost či nepřiměřenost žádosti však v případech pochybností vždy dokládá správce údajů, tedy zaměstnavatel.[39] Možnost odmítnout vyhovět žádosti přímo stanovuje článek 12 Nařízení. Tímto je myšleno na situace, kdy by zaměstnanec (případně bývalý zaměstnanec) požadoval po zaměstnavateli zpřístupnění všech jeho osobních údajů, a to především za účelem zaměstnavateli uškodit a jednalo by se tak z jeho strany o šikanózní

fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 15 až 22.

[38] *Uoou.cz: Práva subjektu údajů* [online]. Změněno 25. 4. 2019. Dostupné z https://www.uoou.cz/6-prava-subjektu-udaju/d-27276.

[39] Tamtéž.

jednání.[40]

Správce údajů se tedy nemusí obávat, že by musel žádostem vyhovět ve sto procentech případů. Ve všech situacích je třeba myslet na princip proporcionality. Tento se používá k řešením takových případů, kdy dojde ke kolizi mezi dvěma či více chráněnými právy. Situaci je třeba posuzovat takovým způsobem, že přednost dostane to právo, které chrání důležitější hodnotu, přičemž ostatní práva musí být omezena jen v co nejmenším rozsahu. Tímto dojde k zachování proporcionality (úměrnosti) mezi jednotlivými, vzájemně si konkurujícími, právy.[41]

7 Sankce

Jedním z možných důsledků porušení povinností dle Nařízení správcem údajů může být podání stížnosti ze strany subjektu údajů k dozorovému orgánu, tedy Úřadu pro ochranu osobních údajů. Na základě takovéto stížnosti ÚOOS následně zahájí šetření a případně správní řízení, jehož předmětem bude zjištění, zda došlo správcem, jehož se stížnost týká, k porušení povinností stanovených mu Nařízením.[42] Úřad má pak při zjištění nedostatků možnost ukládat nápravná opatření. *Každý dozorový úřad má všechny tyto nápravné pravomoci:*

- *upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují Nařízení,*
- *udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily Nařízení,*
- *nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle Nařízení,*
- *nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s Nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě,*

[40] KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018. Strana 94.

[41] KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018. Strana 94.

[42] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 31.

- *nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,*
- *uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,*
- *nařídit opravu či výmaz osobních údajů nebo omezení zpracování a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny,*
- *odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny,*
- *uložit správní pokutu vedle či namísto dalších opatření, podle okolností každého jednotlivého případu,*
- *nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.*[43]

Před účinností Nařízení se v českém prostředí rozpoutala mírná panika, kdy si zaměstnavatelé nebyli jisti, jak přesně se jím mají řídit a co nového se od nich očekává. Primárním důvodem pro jejich obavy byly velice tvrdé sankce nově zavedené Nařízením pro případy porušení povinností z něj vyplývajících. S ohledem na snahu Nařízení sjednotit ochranu osobních údajů napříč celou Unií, jsou sankce taktéž jednotné pro všechny členské státy. Podrobně se jimi zabývá kapitola osmá Nařízení.

[43] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 58 odst. 2.

Dosavadní právní úprava platná v České republice stanovovala maximální hranici při ukládání správních pokut za porušení povinností při ochraně osobních údajů na

10 000 000 Kč.[44] Nařízení tuto částku výrazně navyšuje. Stropem při ukládání správních pokut dle Nařízení je částka 20 000 000 EUR nebo jedná-li se o podnik, až výše 4% celkového celosvětového obratu podniku za předchozí finanční rok, podle toho, která hodnota je vyšší.[45] Při vymezování jednotlivých přestupků je navíc Nařízení poměrně obecné, případně je formuluje jako jakékoli porušení jiných článků Nařízení.

Obrázek 1: Sankce (Zdroj: Eaukcebenefico.cz)

Z pohledu českého prostředí se jedná o velmi vysoké částky, nicméně je třeba mít na paměti, že Nařízení je celoevropským předpisem, které dopadá na správce ze všech unijních zemí, kde sídlí velké společnosti působící na celém světě, pro které by příliš nízké pokuty neměly dostatečný odstrašující účinek.

Při pohledu na takto vysoké částky a vágní formulaci některých přestupků se však nelze divit obavám správců osobních údajů, že případné pokuty pro ně budou zcela likvidační. Tyto obavy se však ÚOOS snaží mírnit. „*Ukládání správních pokut musí být účinné, přiměřené, ale*

[44] § 45 odst. 4 Zákona č. 101/2000 Sb., o ochraně osobních údajů.

[45] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 83 odst. 5.

zároveň odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu. Nikoli za každé porušení obecného nařízení musí být udělena pokuta, ale může být pouze uděleno napomenutí nebo může být správci údajů nařízeno uvést zpracování do souladu s Nařízením atd. Není tak pravdou, že každé porušení obecného nařízení bude představovat uložení správní pokuty."[46]

Představitelé ÚOOS již předem avizovali, že vysokými pokutami chtějí případné hříšníky pouze odrazovat od dalších neplnění povinností, nikoli likvidovat, při jejich udělování pak budou přihlížet k velikosti podniku a závažnosti spáchaného přečinu.[47] V českém prostředí se tedy sankce v maximálních výších uváděných Nařízením nedají předpokládat. Ostatně již zmíněný adaptační zákon tomuto předpokladu vyhověl (viz kapitola 2). Při posuzování výše pokuty bude dále brána v úvahu povaha, závažnost a délka trvání porušení povinností, bude přihlédnuto k povaze, rozsahu a účelu zpracování, počtu dotčených subjektů údajů, a zda se jednalo o úmyslné či nedbalostní porušení.[48] V případě, že správce bude mít za to, že výše jemu uložené pokuty je nepřiměřená, má možnost domáhat se přezkumu její výše, a to v rámci správního soudnictví.[49]

Správní pokuty však nejsou jediné sankce, které správcům osobních údajů hrozí. Kromě jejich udělení totiž „*mohou být správci či zpracovatelé osobních údajů navíc vystaveni žalobám podaným fyzickými osobami s nárokem na náhradu škody v případě hmotné či nehmotné újmy. V neposlední řadě jsou společnosti vystaveny ztrátě důvěry a reputačním rizikům způsobeným nesprávným zacházením s osobními údaji.*"[50] Peněžité sankce jsou tak až zcela posledním prostředkem použitým k vymožení povinností.

Dále nelze opomenout skutečnost, že případy zcela nejzávažnějších porušení povinností v souvislosti se zpracováním osobních údajů mohou být předmětem trestněprávního postihu. Trestný čin neoprávněné nakládání s osobními údaji je v § 180 odst. 1 zákona č. 40/2009, Sb.

---

[46] *Uoou.cz: Sankce, pokuty* [online]. Změněno 25. 4. 2019. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287/p1=4744.

[47] *E15.cz: Šéfka Úřadu pro ochranu osobních údajů: Vysokými pokutami chceme firmy odrazovat, ne likvidovat* [online]. Změněno 25. 5. 2018. Dostupné z: https://www.e15.cz/rozhovory/sefka-uradu-pro-ochranu-osobnich-udaju-vysokymi-pokutami-chceme-firmy-odrazovat-ne-likvidovat-1334926.

[48] *Uoou.cz: Základní příručka k GDPR* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744.

[49] KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. Strana 32.

[50] *GDPR.cz: Sankce* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/.

trestní zákoník, vymezen takto: „*kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.“* Za uvedený trestný čin je možno potrestat také právnickou osobu, a to v souladu s § 7 zákona č. 418/2011, Sb., o trestní odpovědnosti právnických osob a řízení proti nim.

Kromě shora uvedených veřejnoprávních důsledků porušení povinností je třeba zmínit také občanskoprávní odpovědnost správců a zpracovatelů vůči subjektům údajů v rámci smluvních vztahů, a to odpovědnost za vzniklou (hmotnou či nehmotnou) újmu. „*Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy*.“[51] Povinnosti poskytnout náhradu jsou správce a zpracovatel zproštěni v případech, kdy prokáží, že nenesou odpovědnost za událost, která vedla ke vzniku újmy. V opačných případech se poškozený subjekt obrátí s žádostí o náhradu přímo na předmětného správce či zpracovatele, a pokud tento nebude dobrovolně plnit, bude subjekt údajů nucen obrátit se s žalobou na soud.[52]

[51] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Čl. 82 odst. 1.

[52] *Uoou.cz: Základní příručka k GDPR* [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744.

Praktická část

Každá organizace by si primárně měla ujasnit, jaká data zpracovává. K tomuto je třeba provést analýzu odpovídající na danou otázku a dále prověřit systémy, kterými jsou údaje zpracovávány a současně jejich technologické zabezpečení. Na základě takto zjištěných skutečností pak lze přistoupit k dalším opatřením.

V rámci této práce bude zpracována ochrana osobních údajů v návaznosti na Nařízení v organizaci Gymnázium Šternberk.

8 Charakteristika zkoumané organizace

Gymnázium Šternberk je příspěvkovou organizací založenou v roce 1935 pod původním názvem Spolkové československé reálné gymnázium Ústřední matice školské ve Šternberku na Moravě.[53] Činnost gymnázia, přerušená během okupace, byla následně v roce 1945 obnovena a od tohoto roku nepřerušeně funguje dodnes.

Obrázek 2: Hlavní budova školy s hřištěm (zdroj: vlastní)

8.1 Prostorové podmínky a vybavení školy

V roce 1996 došlo z důvodu nedostačujících kapacit školy k rekonstrukci blízké budovy v majetku města, která byla bezplatně převedena do majetku Gymnázia. Propojením nové

[53] *Gymst.com: Historie* [online]. [cit. 12. 6. 2019]. Dostupné z: http://80.gymst.com/index2.html.

přístavby se stávající budovou byla rekonstrukce ukončena a kapacita školy byla zásadně navýšena tak, aby odpovídala vzrůstajícím požadavkům. Areál tedy nyní tvoří dvě budovy, původní budova A a nová budova B. Obě se nachází přímo v historickém centru města. Součástí areálu je dále hřiště přiléhající k budově A a před deseti lety byla postavena nová sportovní hala vzdálená přibližně sto metrů od zbytku areálu školy.

Obrázek 3: Sportovní hala Ecce Homo (zdroj: vlastní)

V současné době je ve škole 36 učeben a laboratoří, z toho je 12 učeben sloužících jako kmenové třídy. Všechny přírodovědné a esteticko-výchovné předměty mají vlastní areály, stejně tak samostatné jsou i jazykové učebny. Součástí školy je také učebna výpočetní techniky. Škola se snaží neustále inovovat a rekonstruovat zařízení. V nedávných letech došlo k zateplení budovy A, rekonstrukci její fasády a výměně oken. V roce 2018 byla zahájena modernizace odborných učeben a laboratoří biologie a chemie. V následujícím období bude mezi priority patřit instalace nového zabezpečovacího systému školy.[54]

[54] Gymnázium Šternberk: Výroční zpráva o činnosti školy ve školním roce 2017/2018. Dostupné online https://cloud5.edupage.org/cloud/Vyrocka_pracovni_rev3.pdf?z%3AaFcNlqO7mPSq1wSnAr3ixpyDP%2FOdqZ5RHQNk9df9nm8vhQ3XFcxSuH1php90MV3%2B.

Obrázek 4: Učebna biologie (zdroj: vlastní)

8.2 Údaje o žácích

Díky velmi dobrým výsledkům u maturit a také při přijímacím řízení na vysoké školy je zájem o studium na Gymnáziu Šternberk vysoký. V loňském roce se na oba obory dohromady hlásilo sto čtyřicet tři uchazečů, přijato jich bylo celkem šedesát.

Z hlediska počtu žáků, kterých je každoročně kolem tři sta padesáti, náleží v rámci Olomouckého kraje ke středně velkým školám. Ve dvou vzdělávacích oborech škola poskytuje střední všeobecné vzdělání končící maturitní zkouškou. Vedle osmiletého oboru škola nabízí také studium čtyřleté. Každoročně se otevírá jedna třída osmiletého oboru a jedna třída čtyřletého oboru. Celkem na škole studují žáci ve dvanácti třídách. Stravování žákům poskytuje jídelna nedaleké Střední odborné školy lesnické a strojní.

Kód oboru	Název oboru	Ukončení studia	Forma studia	Druh studia
79-41-K/41	Gymnázium (čtyřleté)	maturita	denní	úplné střední všeobecné
79-41-K/81	Gymnázium (osmileté)	maturita	denní	úplné střední všeobecné

Tabulka 2: Přehled oborů vzdělávání (zdroj: vlastní)

8.3 Údaje o aktivitách a prezentaci školy

„*Škola je nedílnou součástí aktivit Města Šternberka, většina našich žáků pochází ze Šternberka a blízkého okolí. Gymnázium se zapojuje do většiny akcí pořádaných městem nebo základními školami*.“[55]

Gymnázium upevňuje vztahy se šternberskými základními školami a také dalšími školami v blízkém okolí, velmi dobrá spolupráce je také se Základní uměleckou školou Šternberk a Domem dětí a mládeže Šternberk, kde se žáci úspěšně účastní soutěží. Gymnázium Šternberk je fakultní školou Přírodovědecké fakulty UP Olomouc, jejichž aktivit se pravidelně účastní. Žáci každoročně jezdívají na různé vzdělávací pobyty.

Významným partnerem školy je Město Šternberk, které škole poskytuje pomoc při různých akcích a poskytuje příspěvky na aktivity. Tradičně dobrou spolupráci má škola také s Hradem Šternberk, jehož prostory jsou využívány při akcích školy, jako je imatrikulace, předávání maturitních vysvědčení a dalších kulturních akcí, příkladem mohou být Svatomartinské slavnosti, které škola každoročně organizuje, a jsou ve Šternberku velice populární, účastní se jich mnoho obyvatel města všech věkových kategorií. Prostřednictvím O.p.s. rodičů a příznivců Gymnázia Šternberk jsou podporováni nejlepší studenti formou sponzorských darů od místních firem.

V rámci projektu Erasmus Plus škola dlouhodobě spolupracuje se zahraničními středními školami, a to v Belgii, Lucembursku, Holandsku, Německu a Francii, kdy jsou organizovány výměnné pobyty pro žáky i zaměstnance.

Gymnázium se intenzivně snaží o svou propagaci, každoročně se prezentuje na veletrhu středních škol Scholaris, pro absolventy školy, zájemce o studium a také pro obyvatele města jsou pořádány dny otevřených dveří, kde se může veřejnost seznámit jednak s interiéry budovy, ale také současnými žáky, kteří prezentují aktivity školy.

8.4 Personální zabezpečení a organizační struktura

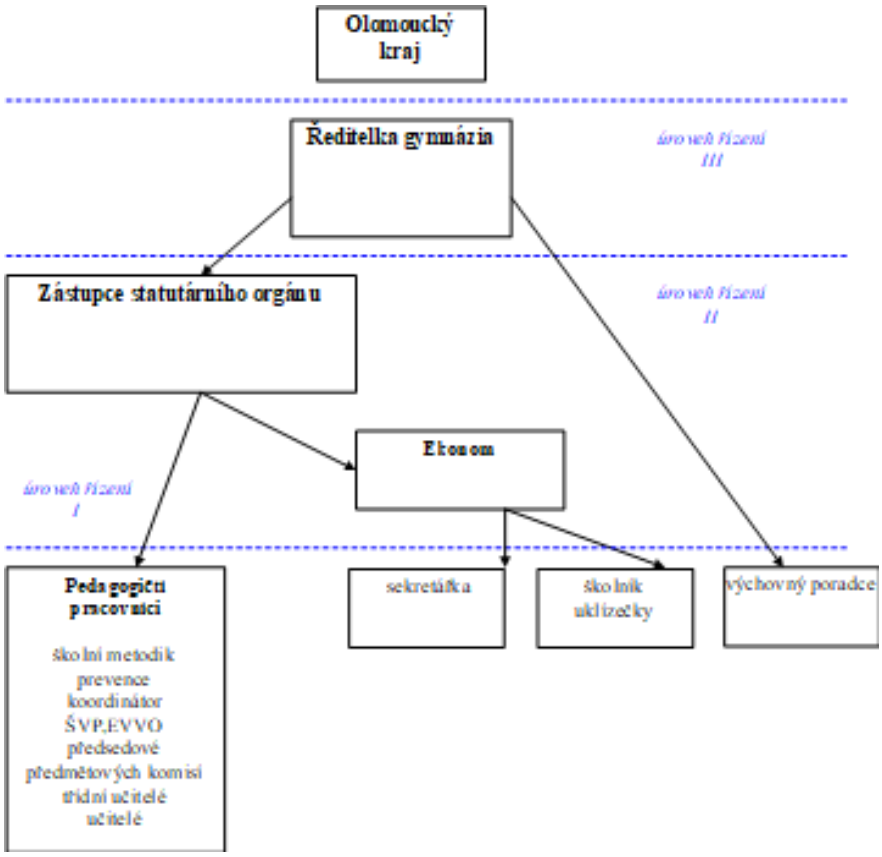
Statutárním orgánem příspěvkové organizace je ředitel, jmenovaný Radou Olomouckého kraje. Ředitel řídí školu, plní povinnosti vedoucího organizace a další úkoly vyplývající z obecně závazných právních předpisů. Jmenuje a odvolává svého zástupce, který ho

[55] Gymnázium Šternberk: Výroční zpráva o činnosti školy ve školním roce 2017/2018. Dostupné online https://cloud5.edupage.org/cloud/Vyrocka_pracovni_rev3.pdf?z%3AaFcNlqO7mPSq1wSnAr3ixpyDP%2FOdqZ5RHQNk9df9nm8vhQ3XFcxSuH1php90MV3%2B.

zastupuje v době jeho nepřítomnosti.[56]

Gymnázium zaměstnává celkem třicet pět pedagogických pracovníků (z toho pět na mateřské dovolené) a osm nepedagogických pracovníků (ekonomka, administrativní pracovnice, školník a pět uklízeček). Na škole působí výchovná poradkyně, metodik prevence a na částečný úvazek také psycholog, jejichž úkolem je zajistit prevenci rizikového chování a starat se o duševní zdraví žáků, pedagogů a dalších zaměstnanců.

Organizační struktura je znázorněna na obrázku č. 5.[57]



Obrázek 5: Organizační struktura školy

[56] Zřizovací listina Gymnázia Šternberk ze dne 19.12.2016

[57] Vnitřní organizační řád Gymnázia Šternberk, platnost od 1.2.2013

9 Analýza situace v oblasti zpracování osobních údajů ve zkoumané organizaci

Hlavní náplní organizace jako správce údajů, je výkon veřejné správy na úseku školství podle zákona č. 561/2004Sb., školského zákona a dalších právních předpisů. V rámci této činnosti dochází k nakládání s osobními údaji několika různých skupin osob. Primárně se však jedná o zpracování údajů zaměstnanců školy a jejích studentů. S těmito údaji organizace zachází v poměrně značném rozsahu. Mimo dané skupiny zachází také s údaji dodavatelských subjektů, ale již v menším rozsahu.

Analýza situace v oblasti zpracování osobních údajů ve zkoumané organizaci byla provedena ve dvou krocích. Nejdříve v součinnosti s ředitelkou školy Mgr. Tamarou Kaňákovou, a to formou rozhovoru, kdy byly zjištěny podrobnosti o oblastech a způsobech zpracování osobních údajů v organizaci a opatření učiněná v organizaci po účinnosti GDPR. Dalším krokem bylo dotazníkové šetření se zaměstnanci školy s dotazy zaměřenými také na tuto oblast.

Přehled všech činností, při nichž dochází ke zpracování osobních údajů, je následující:

- personální a mzdová agenda,
- účetní agenda,
- spisová služba,
- evidence smluv,
- agenda zadávání veřejných zakázek,
- provozování webových stránek a propagace školy,
- přijímací řízení,
- vedení školní matriky a třídních knih,
- evidence úrazů a BOZP,
- agenda související s ukončením vzdělávání,
- reakce na dožádání orgánu veřejné moci,
- ostatní pedagogicko-správní agenda.

Jednotlivé činnosti zpracování osobních údajů jsou rozděleny do tří kategorií dle postavení zkoumaných subjektů, a to na agendu zpracování osobních údajů zaměstnanců, zpracování osobních údajů studentů a zpracování osobních údajů v dodavatelsko-odběratelských vztazích.

9.1 Zpracování osobních údajů zaměstnanců školy

Pod tuto kategorii lze zařadit personální a mzdovou agendu, evidenci úrazů a reakce na dožádání orgánu veřejné moci.

Personální a mzdovou agendou se rozumí především shromažďování osobních údajů zaměstnanců za účelem naplňování pracovně-právních vztahů, tedy vedení pracovní dokumentace, osobních spisů zaměstnanců, zajištění vstupní a preventivní lékařské prohlídky zaměstnanců, shromažďování údajů o dosaženém vzdělání, zjišťování a zakládání historie trestní minulosti (výpis z rejstříku trestů), potvrzení o pracovní neschopnosti a prohlášení poplatníka k dani z příjmu ze závislé činnosti. V souvislosti s uvedenými činnostmi zaměstnavatel shromažďuje tyto osobní údaje zaměstnanců: jméno a příjmení, titul, datum narození, adresa, rodné číslo, telefonní číslo, místo a stát narození, státní příslušnost, číslo zdravotní pojišťovny, číslo bankovního účtu, údaje o předchozích zaměstnavatelích, rodině a dětech, shromažďuje platové výměry zaměstnanců. Tyto osobní údaje jsou shromažďovány v souladu se zákonem č. 262/2006 Sb., zákoník práce a zákonem č. 563/2004 Sb., o pedagogických pracovnících a zákonem č. 586/1992 Sb. o daních z příjmu, a proto není vyžadován souhlas zaměstnanců s jejich sběrem a zpracováním. V rámci této agendy jsou zpracovávány citlivé údaje zaměstnanců (údaje o rodinných příslušnících – dětech, zdravotní údaje). Veškerou tuto agendu zpracovává ekonomka školy, přístup k těmto informacím má dále ředitelka školy a její zástupce. Žádná další osoba není autorizovaná k přístupu k daným informacím. Informace jsou uchovávány jednak v listinné podobě a dále jsou uchovávány v elektronické formě, mzdová agenda je pak zpracovávána na osobním počítači ekonomky v mzdovém programu PERM od společnosti Kvasar, spol. s.r.o. Komunikace s veškerými úřady probíhá prostřednictvím datové schránky. Přístup k ní mají ředitelka, ekonomka a administrativní pracovnice (sekretářka). Osobní spisy zaměstnanců v papírové formě jsou uchovávány v uzamykatelných skříních v kanceláři ekonomky. Likvidaci a proplácení cestovních příkazů zajišťuje administrativní pracovnice školy.

Co se týče **reakce na dožádání orgánů veřejné moci**, tato je zde taktéž založena. Na

tyto dotazy odpovídá úřadům opět ekonomka školy. Jedná se především o poskytnutí součinnosti soudu či soudním exekutorům. Na příklad jde o situace, kdy je mzda některého ze zaměstnanců postižena exekučním příkazem, případně je třeba potvrdit soudu příjem zaměstnance k soudnímu řízení.

Kniha pracovních úrazů je uchovávána v kanceláři ekonomky v papírové podobě, v posledních deseti letech nebyl žádný pracovní úraz řešen.

Agenda BOZP, která sestává z dokumentů o proškolení a profesní způsobilosti zaměstnanců, je evidována a založena v kanceláři zástupce ředitelky v uzamykatelné skříni.

9.2 Zpracování osobních údajů studentů školy

Vzhledem k hlavní činnosti zkoumané organizace, kterou je vzdělávání, dochází ke shromažďování a následnému uchovávání osobních údajů studentů školy a jejich zákonných zástupcích.

Tyto činnosti začínají vedením **přijímacího řízení**, při němž se evidují a zakládají v listinné formě přihlášky ke studiu, rozhodnutí o přijetí nebo nepřijetí studenta a zápisové lístky centrálně do uzamykatelného prostoru.

Po celou dobu školní docházky se vede **evidence žáků ve školní matrice** a záznamy o docházce jsou evidovány v třídních knihách. Dalšími důležitými dokumenty o studentech jsou zprávy a doporučení k poskytnutí podpůrných opatření, tyto zakládá v listinné podobě výchovná poradkyně a uchovává v uzamykatelné skříni ve své kanceláři.

K evidenci úrazů studentů slouží **kniha úrazů**, uložená na sekretariátě školy. Pro uplatnění odškodnění zajišťuje administrativní pracovnice komunikaci s pojišťovnami a ČŠI a veškeré originální doklady související s touto agendou jsou uloženy v uzamykatelné skříni centrálně na jednom místě na sekretariátě.

Ostatní **pedagogicko-správní agenda** zahrnuje potvrzení o době studia, žádosti o uvolnění z výuky, protokoly o komisionálních zkouškách, agendu související s ukončením vzdělání, tedy vydávání maturitních vysvědčení a doklady o maturitní zkoušce, evidenci stížností žáků nebo jejich zákonných zástupců. U všech těchto činností dochází ke zpracování zvláštní kategorie osobních údajů tzv. citlivých údajů, jelikož subjektem osobních údajů je dítě a zdravotní údaje.

O studentech jsou v souladu se zákonem č. 561/2004 Sb., zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), vyhláškou č. 353/2016 Sb., vyhláška o přijímacím řízení ke střednímu vzdělávání, vyhláškou č.

364/2005 Sb., vyhláška o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky (vyhláška o dokumentaci škol a školských zařízení), vyhláškou č. 177/2009 Sb., vyhláška o bližších podmínkách ukončování vzdělávání ve středních školách maturitní zkouškou a dále v souladu se zákonem č. 500/2004 Sb., správní řád shromažďovány následující informace: jméno a příjmení, datum narození, rodné číslo, místo trvalého pobytu, místo a stát narození, státní občanství, doručovací adresa, závěr o zdravotní způsobilosti ke vzdělávání, informace o schopnostech a zájmech a stupeň podpůrných opatření. Tyto informace jsou součástí přihlášky ke vzdělávání, jsou tedy shromažďovány už u uchazečů o přijetí ke studiu. Zůstávají založeny i v případě, že uchazeč není ke studiu přijat. S ohledem na nezletilost žáků jsou shromažďovány také informace o jejich zákonných zástupcích, tedy jejich jméno a příjmení, datum narození, adresa, telefonní číslo, e-mailový kontakt.

Všechny tyto informace o studentech a jejich zákonných zástupcích jsou ukládány v listinné podobě centrálně na sekretariátě školy, kde k nim má přístup omezený počet pověřených osob. Kopie některých informací jsou také založeny v osobních spisech studentů u jejich třídních učitelů. Dále jsou informace uloženy digitálně, školní matrika je zpracovávána v elektronickém systému EduPage. Provozovatelem této služby je obchodní společnost aScApplied Software Consultants s.r.o. Jedná se o cloudový typ služby, data jsou tedy uložena u externí společnosti. Program je instalován na vzdáleném serveru ve formě webové služby. Přístup do aplikace je chráněn unikátním přihlašovacím jménem a heslem pro jednotlivé uživatele. Ze strany gymnázia je aplikován řízený přístup k osobním údajům. To znamená, že uživatelské účty jsou rozlišeny na správcovské (nejvyšší oprávnění – tímto disponuje pouze zástupce ředitelky), na třídní učitele (tito mají právo aktualizovat zde osobní údaje studentů a jejich zákonných zástupců a evidují docházku), ostatní učitele (tito mají pouze oprávnění zapisovat zde hodnocení studentů) a administrativní pracovnici školy (má oprávnění evidovat údaje související s přijímacím řízením).

9.3 Zpracování osobních údajů v dodavatelsko-odběratelských vztazích

V rámci dodavatelsko-odběratelských vztahů dochází ke zpracování údajů dalších osob v účetní agendě, evidenci smluv, v rámci spisové služby a při zadávání veřejných zakázek.

V **účetní** agendě jsou shromažďovány podklady pro účetnictví v listinné podobě dle zákona 563/1991 Sb., o účetnictví (faktury, příjmové doklady apod.) v šanonech v kanceláři ekonomky. Kancelář je uzamykatelná. Pro vedení účetnictví je využíván program Fenix od

firmy Asseco Solutions a.s., nainstalován na počítačích dvou uživatelů, ekonomky a administrativní pracovnice. Přístup do aplikace je chráněn unikátním přihlašovacím jménem a heslem pro jednotlivé uživatele. PC stanice jsou umístěny v uzamykatelných místnostech. Probíhá zde řízený přístup do systému ze strany k tomu oprávněných osob.

Evidence smluv s dodavateli a odběrateli jsou uloženy v listinné podobě v šanonech v kanceláři administrativní pracovnice. Zároveň smlouvy, u kterých to ukládá zákon č. 340/2015 Sb., o registru smluv, jsou zveřejňovány v souladu s tímto zákonem ekonomkou školy v součinnosti s administrativní pracovnicí.

Spisovou službu zajišťuje administrativní pracovnice. Na základě schváleného archivačního a skartačního řádu školy (sestaveným v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě a závazným pokynem zřizovatele) přiřazuje jednotlivým dokumentům skartační znaky. Dokumentace je fyzicky uložena v uzamykatelných prostorech na sekretariátu a jejich elektronická evidence probíhá prostřednictvím systému GINIS od zprostředkovatele GORDIC spol. s r.o. Přístup do systému je chráněn unikátním jménem a heslem pro jednotlivé uživatele.

Zadávací řízení **veřejných zakázek** zahrnuje evidenci listinných dokumentů v šanonech v uzamykatelných prostorech a digitální zadávání veřejných zakázek přes portál. PC stanice je umístěna v uzamykatelné kanceláři. V rámci těchto činností jsou zpracovávány následující osobní údaje: jméno a příjmení, datum narození, IČ, DIČ, bydliště, trvalý pobyt, sídlo/adresa provozovny, číslo bankovního účtu, ID datové schránky, telefonní číslo, e-mail, podpis. V rámci těchto agend nedochází ke zpracovávání citlivých osobních údajů.

9.4 Opatření v organizaci po účinnosti GDPR

V souvislosti s přijetím nařízení GDPR byla v předmětné organizaci přijata následující opatření:

1. Vzhledem k tomu, že se jedná o organizaci shromažďující osobní údaje dle článku 37 Nařízení, tedy je Správce vykonavatelem veřejné správy, vznikla jí povinnost ustanovit pověřence pro ochranu osobních údajů. Proto byla uzavřena smlouva o poskytování služeb pověřence s organizací Schola Servis GDPR, s.r.o., zastoupenou JUDr. Ing. et Ing. Romanem Ondrýskem, Ph.D. MBA, kterou se pověřenec zavazuje k plnění všech povinností dle Nařízení. Na webových stránkách školy byly zveřejněny údaje o pověřenci a prohlášení o ochraně osobních údajů (příloha č. 1). Kontaktní údaje pověřence byly dále sděleny Úřadu pro ochranu osobních údajů.

2. Byla aktualizována směrnice o ochraně osobních údajů.
3. Zaměstnanci byly poučeni o zásadách mlčenlivosti o všech skutečnostech, o nichž se v rámci výkonu své práce dozvědí, a to po dobu trvání pracovního poměru i po jeho skončení (viz příloha č. 2).
4. Zaměstnanci byly proškoleni o kybernetické bezpečnosti a zabezpečení dat ve škole.
5. Byl sepsán seznam zaměstnanců dle jejich přístupu do jednotlivých místností a byly doplněny uzamykatelné skříňky do kabinetů.
6. Byly aktualizovány formuláře se souhlasy se zpracováním osobních údajů pro nezletilé žáky a jejich zákonné zástupce (viz příloha č. 3) a pro zletilé žáky (viz příloha č. 4).
7. Bylo zrušeno vedení třídních knih v papírové formě, aby se zabránilo možnosti nahlížet do nich ve třídách.
8. Bylo zrušeno zveřejňování fotodokumentace ze školních akcích na sociálních sítích (facebook, rajče.net).
9. Byly sepsány zpracovatelské smlouvy ve smyslu článku 28 odst. 3 Nařízení s těmito zpracovateli, kteří poskytují Gymnáziu Šternberk služby, při nichž dochází ke zpracování osobních údajů:
    - aScApplied Software Consultantss.r.o.

      poskytuje služby webhostingu a softwarové služby pro vedení elektronické pedagogické agendy.
    - MERIT GROUP a.s.

      poskytuje IT služby (například dodání knihovního systému, správa serveru apod.).
    - AssecoSolutions, a.s.

      je využíván programový software zpracovatele při vedení účetnictví.
    - Kvasar, spol. s r. o.

      je využíván programový software zpracovatele při vedení mzdového účetnictví.
    - GORDIC spol. s r.o.

      je využíván programový software zpracovatele při vedení elektronické spisové služby.
    - STUDENT AGENCY k.s.

      na základě smlouvy o zájezdu poskytuje studentům a zaměstnancům Gymnázia Šternberk služby cestovního ruchu.

9.5 Dotazníkové šetření

Dalším krokem analýzy je dotazníkové šetření mezi zaměstnanci Gymnázia Šternberk. V rámci dotazníkového šetření byli osloveni všichni zaměstnanci Gymnázia Šternberk, kteří při své pracovní činnosti zpracovávají osobní údaje ve smyslu čl. 4 Nařízení, což činí 30 učitelů, výchovná poradkyně, metodik prevence, psycholog, ekonomka a administrativní pracovnice školy, tj. celkem 35 osob.

Otázky byly zaměřeny na zjištění pracovní pozice, obsahu a rozsahu zpracovávaných osobních údajů v rámci jednotlivých agend v organizaci, používání technických prostředků, způsob zabezpečení a hodnocení navýšení pracovních povinností v souvislosti se zavedením GDPR.

Dotazníkové šetření bylo provedeno elektronickou formou prostřednictvím serveru survio.cz. Všem osloveným byl zaslán odkaz k vyplnění dotazníku:

https://www.survio.com/survey/d/U6R6I9X0T0A7P5H7K

9.5.1 Ukázka dotazníku

Dotazníkové šetření zaměstnanců Gymnázia Šternberk v oblasti zpracování osobních údajů

Dobrý den,

věnujte prosím několik minut svého času vyplnění následujícího dotazníku.

1. Jakou pracovní pozici v organizaci zastáváte?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Učitel
- ◯ Výchovný poradce, metodik prevence, psycholog
- ◯ Ekonom nebo administrativní pracovník

2. Při své práci zpracováváte osobní údaje kterých subjektů?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Nezletilých žáků
- ☐ Zákonných zástupců žáků nebo zletilých žáků
- ☐ Zaměstnanců a jejich rodinných příslušníků
- ☐ Dodavatelů a odběratelů služeb a zboží

3. Jaké osobní údaje výše uvedených subjektů zpracováváte?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Obecné osobní údaje: jméno, pohlaví, věk a datum narození, osobní stav, fotografický záznam
- ☐ Údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání
- ☐ O zdravotním stavu
- ☐ Genetické, biometrické údaje

4. Jaké technické prostředky používáte ke zpracování osobních údajů?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ PC nebo notebook
- ☐ USB flash disk/externí disk
- ☐ Digitální fotoaparát
- ☐ Papírové nosiče
- ☐ Vnitřní server – intranet
- ☐ Mobilní telefon

5. Používáte při zabezpečení osobních počítačů nebo notebooků standartní bezpečné přístupové heslo (např. stávající se z osmi znaků v kombinaci velkých a malých písmen a číslic)?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Ano
- ◯ Ne

6. Používáte v případě zveřejňování osobních údajů prvky pseudonymizace nebo anonymizace? (např. při zveřejňování výsledků z přijímacího řízení, komunikaci se školským poradenským zařízením, apod.)

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Ano
- ◯ Ne
- ◯ Otázka se mě vzhledem k náplni mé práce netýká

7. Jakým způsobem máte zabezpečeny osobní údaje v listinné podobě?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ V uzamykatelné skříni
- ◯ V uzamykatelné skříni a uzamykatelné kanceláři
- ◯ V uzamykatelné místnosti bez dalšího zabezpečení
- ◯ Nejsou zabezpečeny

8. Vznikly Vám v souvislosti se zavedením GDPR nějaké nové povinnosti?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ ano
- ◯ ne

9. Nakolik hodnotíte časové navýšení administrativní práce po zavedení GDPR ?

Nápověda k otázce: *Vyberte jednu odpověď*

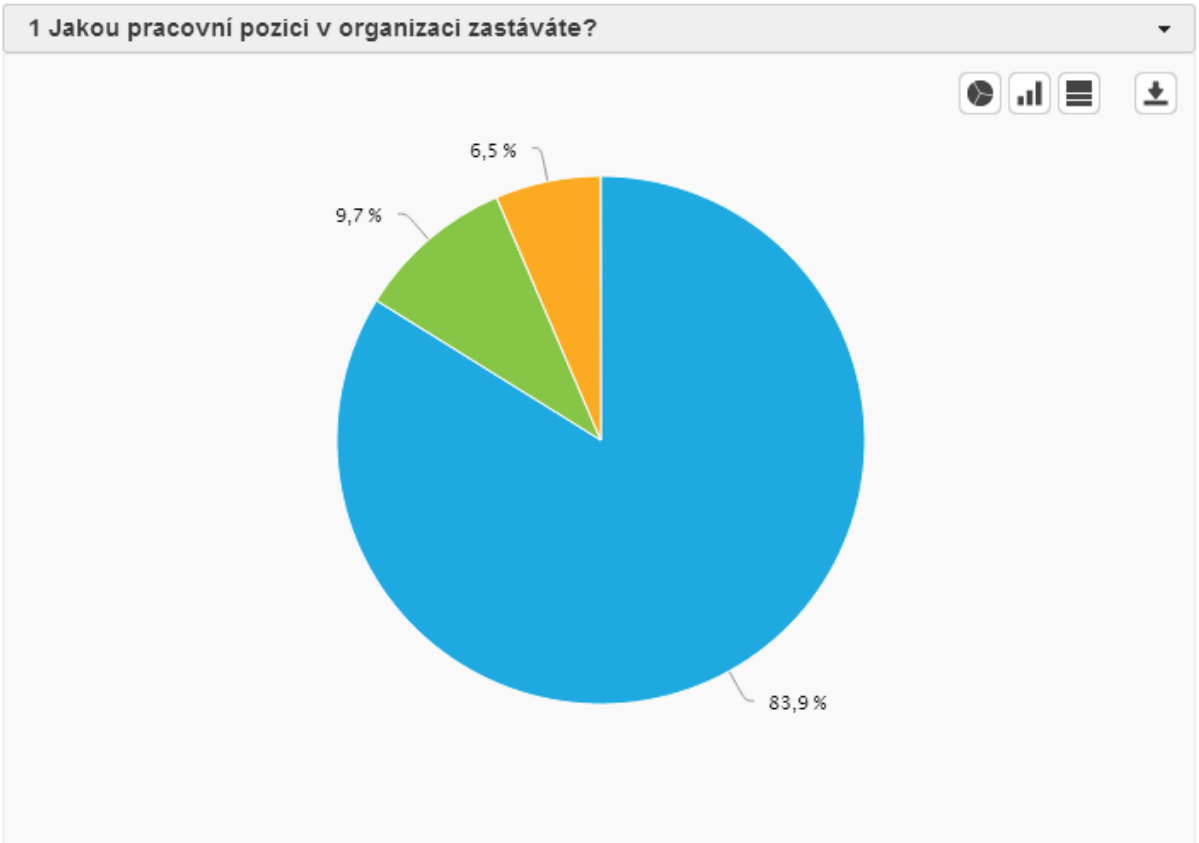
- ◯ Získávání a zajišťování osobních údajů je výrazně časově náročnější, než před zavedením GDPR
- ◯ Nevidím výraznější časové navýšení, ale náročnější je vlastní organizace získávání a zpracování osobních údajů
- ◯ Časová náročnost je přibližně stejná, nevnímám výrazný rozdíl

10. Považujete stávající zabezpečení ochrany osobních údajů ve vámi zpracovávané agendě za dostatečné?

Nápověda k otázce: *Vyberte jednu odpověď*

- ◯ Ano
- ◯ Ne - doplňte: [ ]

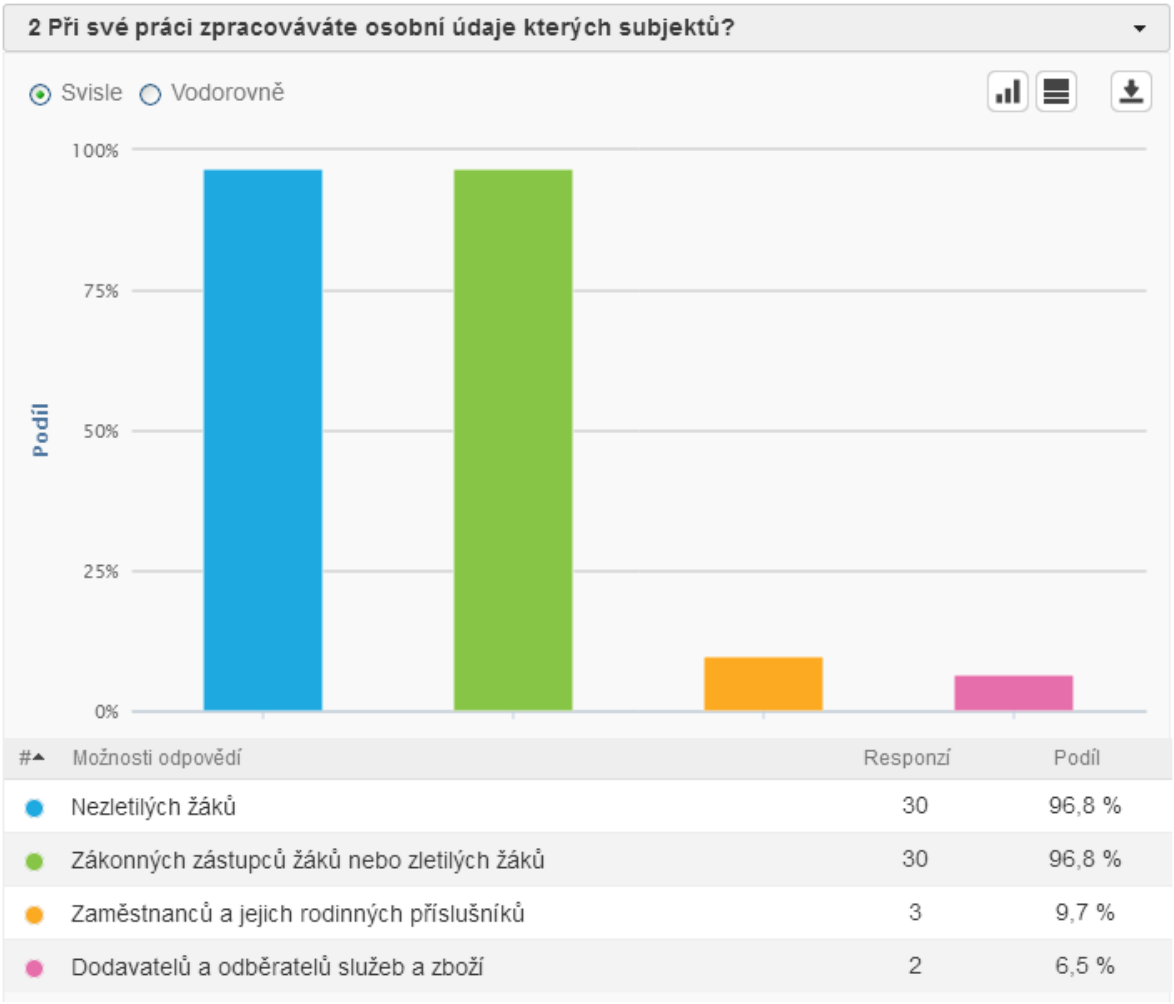
9.5.2 Otázky a odpovědi v dotazníkové šetření



#	Možnosti odpovědí	Responzí	Podíl
●	Učitel	26	83,9 %
●	Výchovný poradce, metodik prevence, psycholog	3	9,7 %
●	Ekonom nebo administrativní pracovník	2	6,5 %

Graf 1: Odpovědi na otázku č. 1

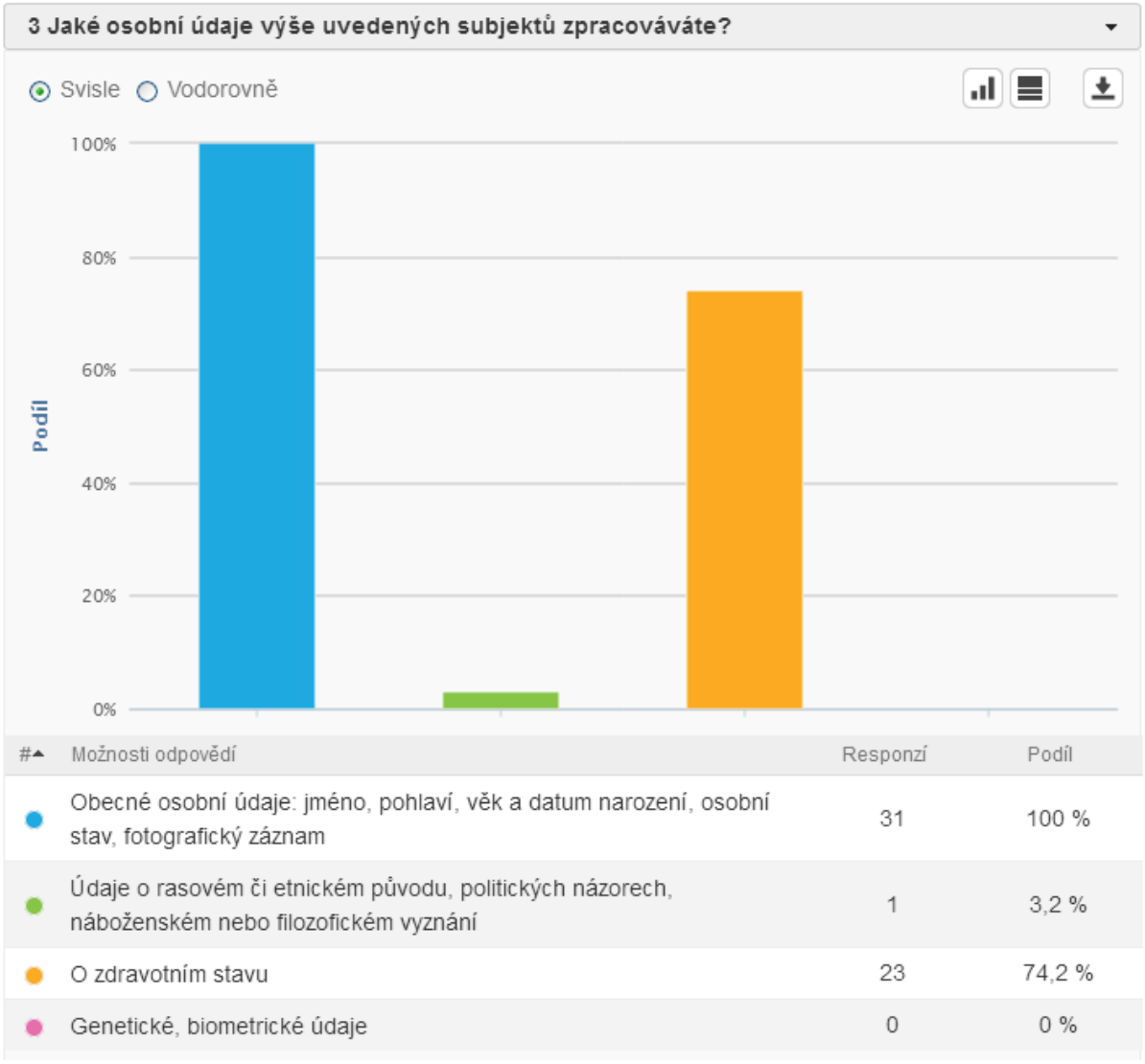
Z celkové počtu 35 oslovených zaměstnanců Gymnázia Šternberk vyplnilo dotazníky 31 respondentů, z toho 26 učitelů, výchovná poradkyně, metodik prevence, psycholog a 2 zaměstnanci ekonomického úseku, tj. 88,57% všech zaměstnanců, kteří při výkonu své práce zpracovávají osobní údaje jiných osob.



#	Možnosti odpovědí	Responzí	Podíl
●	Nezletilých žáků	30	96,8 %
●	Zákonných zástupců žáků nebo zletilých žáků	30	96,8 %
●	Zaměstnanců a jejich rodinných příslušníků	3	9,7 %
●	Dodavatelů a odběratelů služeb a zboží	2	6,5 %

Graf 2: Odpovědi na otázku č. 2

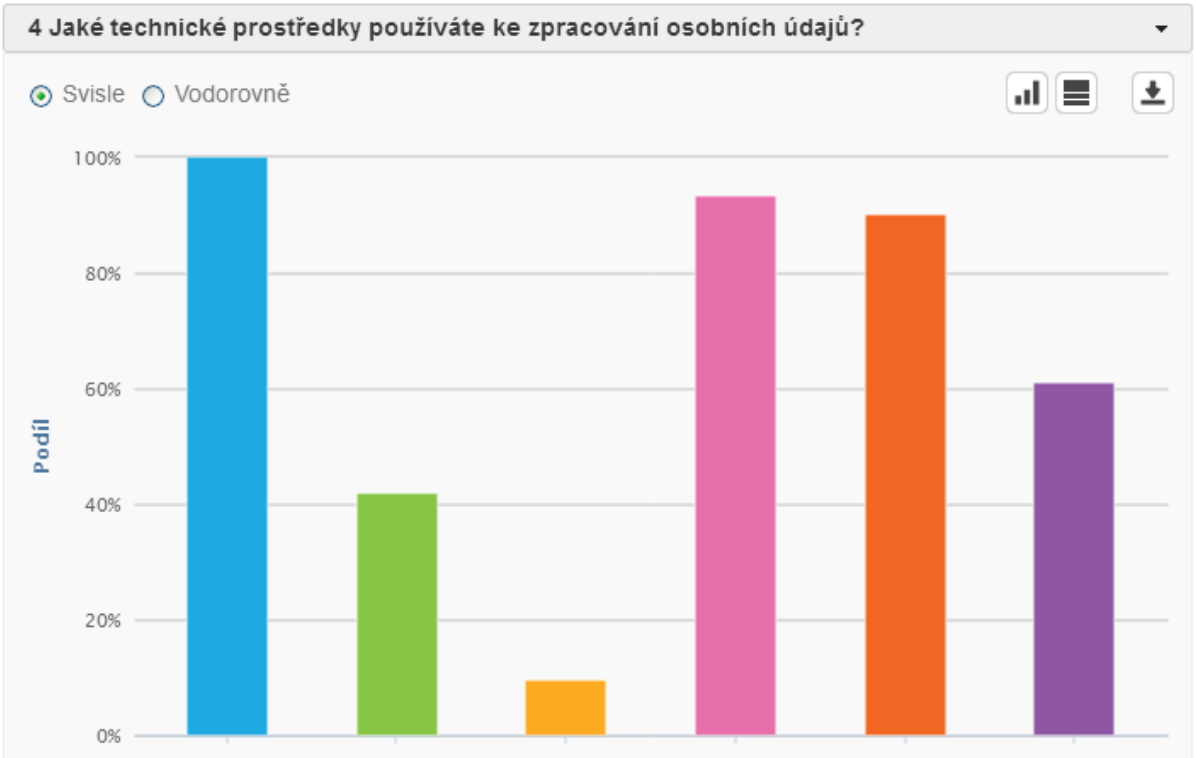
Téměř všichni respondenti zpracovávají osobní údaje nezletilých žáků, jejich zákonných zástupců a zletilých žáků, což jsou všichni učitelé, výchovná poradkyně, metodik prevence, psycholog a administrativní pracovnice školy. Osobní údaje zaměstnanců zpracovávají pouze 3 zaměstnanci, u kterých to vyplývá z jejich náplně práce, ekonomka v rámci personální a mzdové agendy, administrativní pracovnice při likvidaci cestovních příkazů a zástupce ředitelky jako přímý nadřízený pracovník pedagogického sboru. Agendami v oblasti dodavatelsko-odběratelských vztahů se zabývají pouze 2 zaměstnanci ekonomického úseku.



#	Možnosti odpovědí	Responzí	Podíl
●	Obecné osobní údaje: jméno, pohlaví, věk a datum narození, osobní stav, fotografický záznam	31	100 %
●	Údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání	1	3,2 %
●	O zdravotním stavu	23	74,2 %
●	Genetické, biometrické údaje	0	0 %

Graf 3: Odpovědi na otázku č. 3

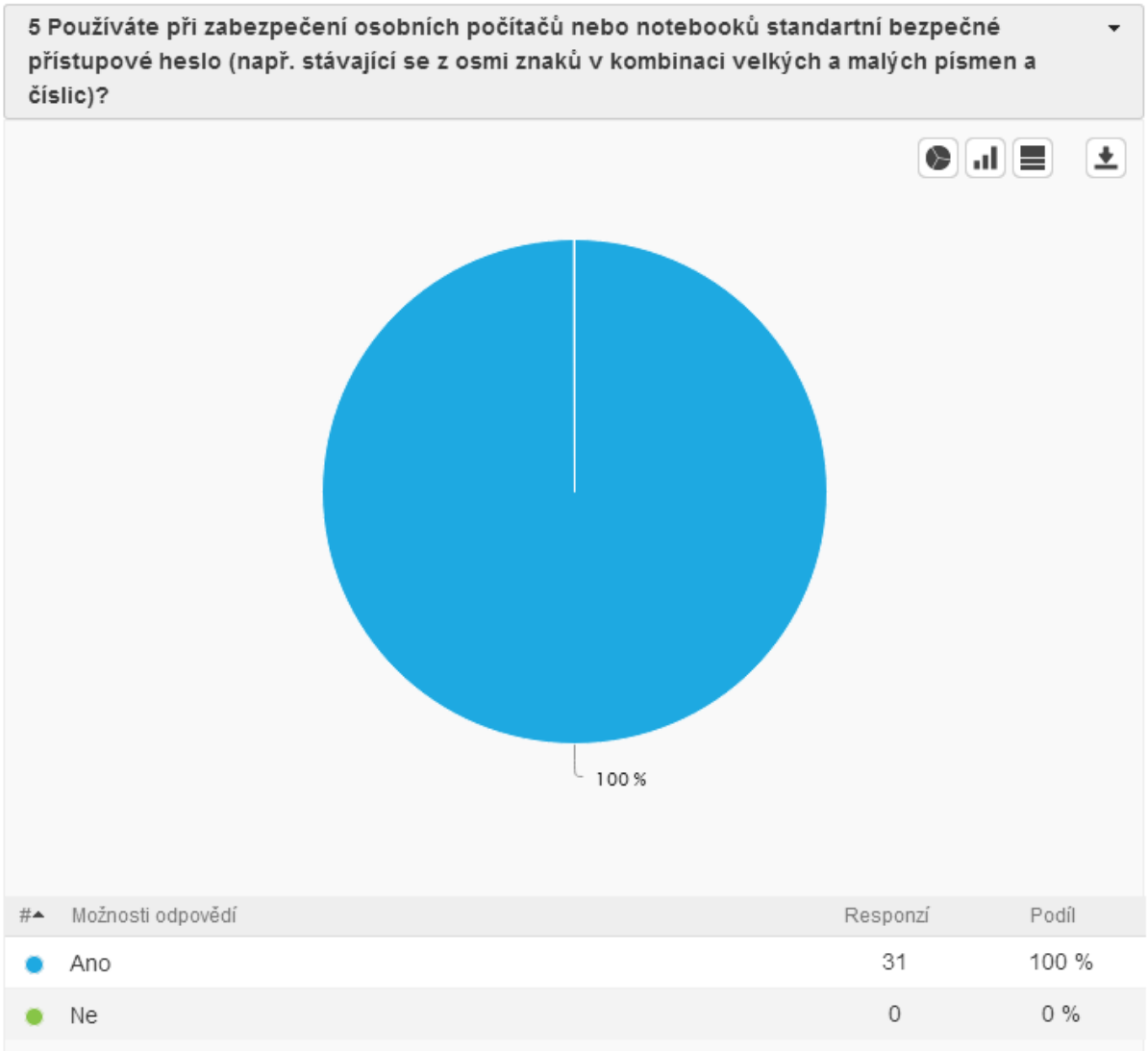
Všichni respondenti odpověděli, že při své práci zpracovávají obecné osobní údaje a většina z nich i údaje o zdravotním stavu, pouze výchovná poradkyně může přijít při své práci k údajům o rasovém či etnickém původu.



#	Možnosti odpovědí	Responzí	Podíl
1	PC nebo notebook	31	100 %
2	USB flash disk/externí disk	13	41,9 %
3	Digitání fotoaparát	3	9,7 %
4	Papírové nosiče	29	93,5 %
5	Vnitřní server –intranet	28	90,3 %
6	Mobilní telefon	19	61,3 %

Graf 4: Odpovědi na otázku č. 4

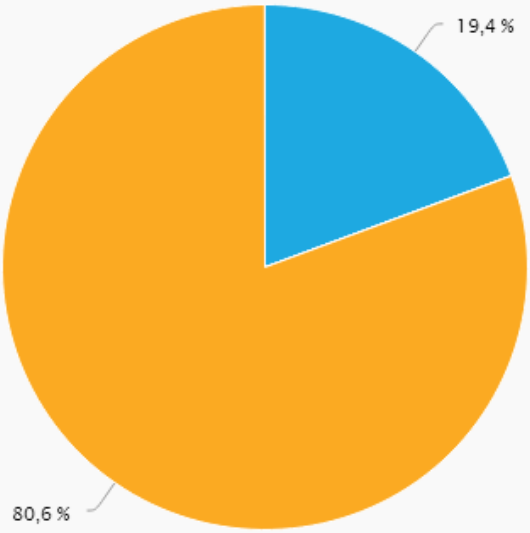
Všichni respondenti ke zpracování osobních údajů používají počítač nebo notebook a spolu s ním téměř všichni ještě papírové listiny a intranet. Někteří učitelé využívají k uchování dat USB flash disk nebo externí disk a 3 učitelé mají na starosti fotodokumentování školních akcí, proto také využívají digitální fotoaparát. Z dotazníku vyplynulo, že více než polovina učitelů užívá ke zpracování osobních údajů žáků svůj mobilní telefon.



Graf 5: Odpovědi na otázku č. 5

Všichni respondenti zabezpečují své notebooky a počítače bezpečným heslem.

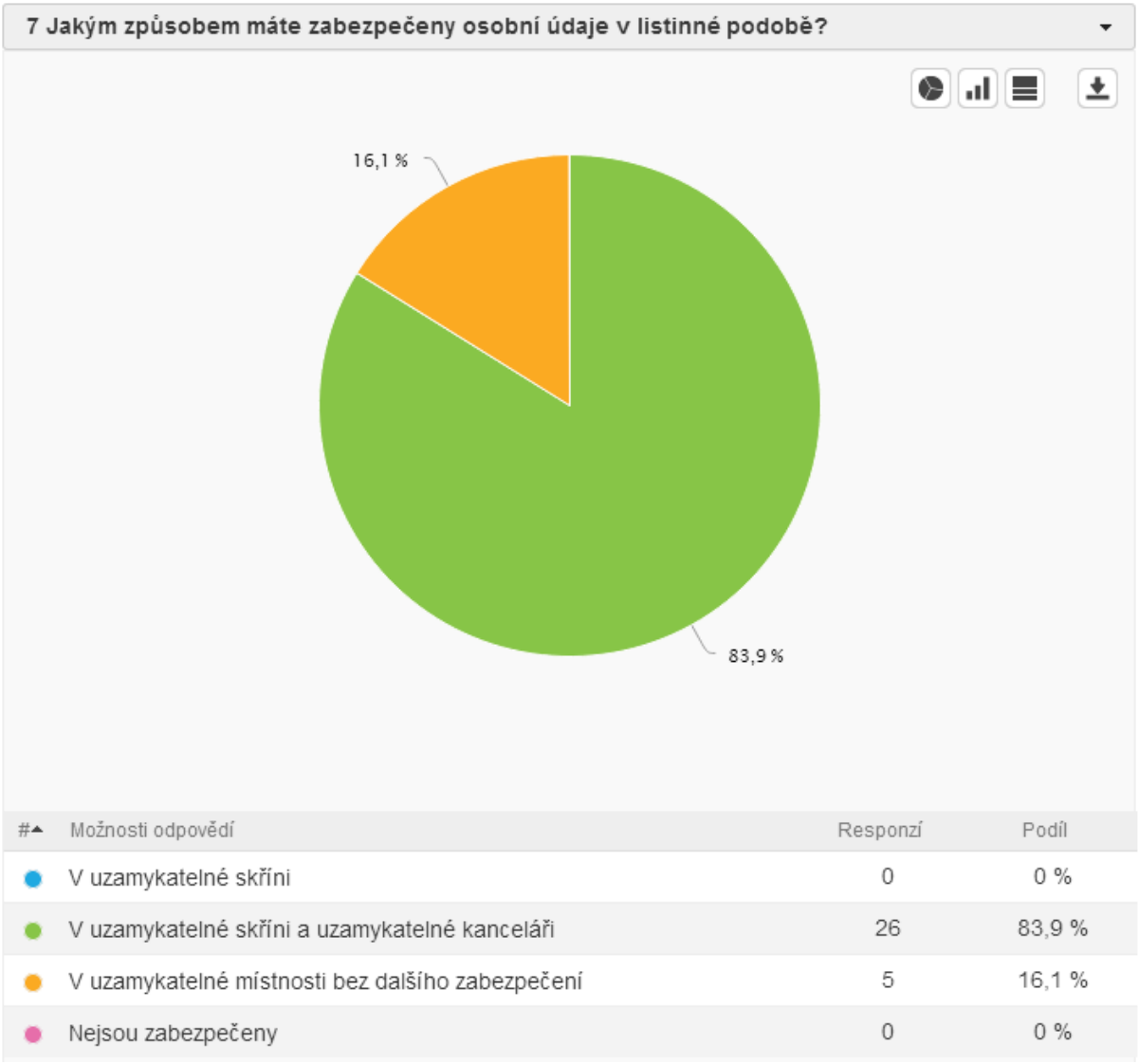
6 Používáte v případě zveřejňování osobních údajů prvky pseudonymizace nebo anonymizace? (např. při zveřejňování výsledků z přijímacího řízení, komunikaci se školským poradenským zařízením, apod.)



#	Možnosti odpovědí	Responzí	Podíl
●	Ano	6	19,4 %
●	Ne	0	0 %
●	Otázka se mě vzhledem k náplni mé práce netýká	25	80,6 %

Graf 6: Odpovědi na otázku č. 6

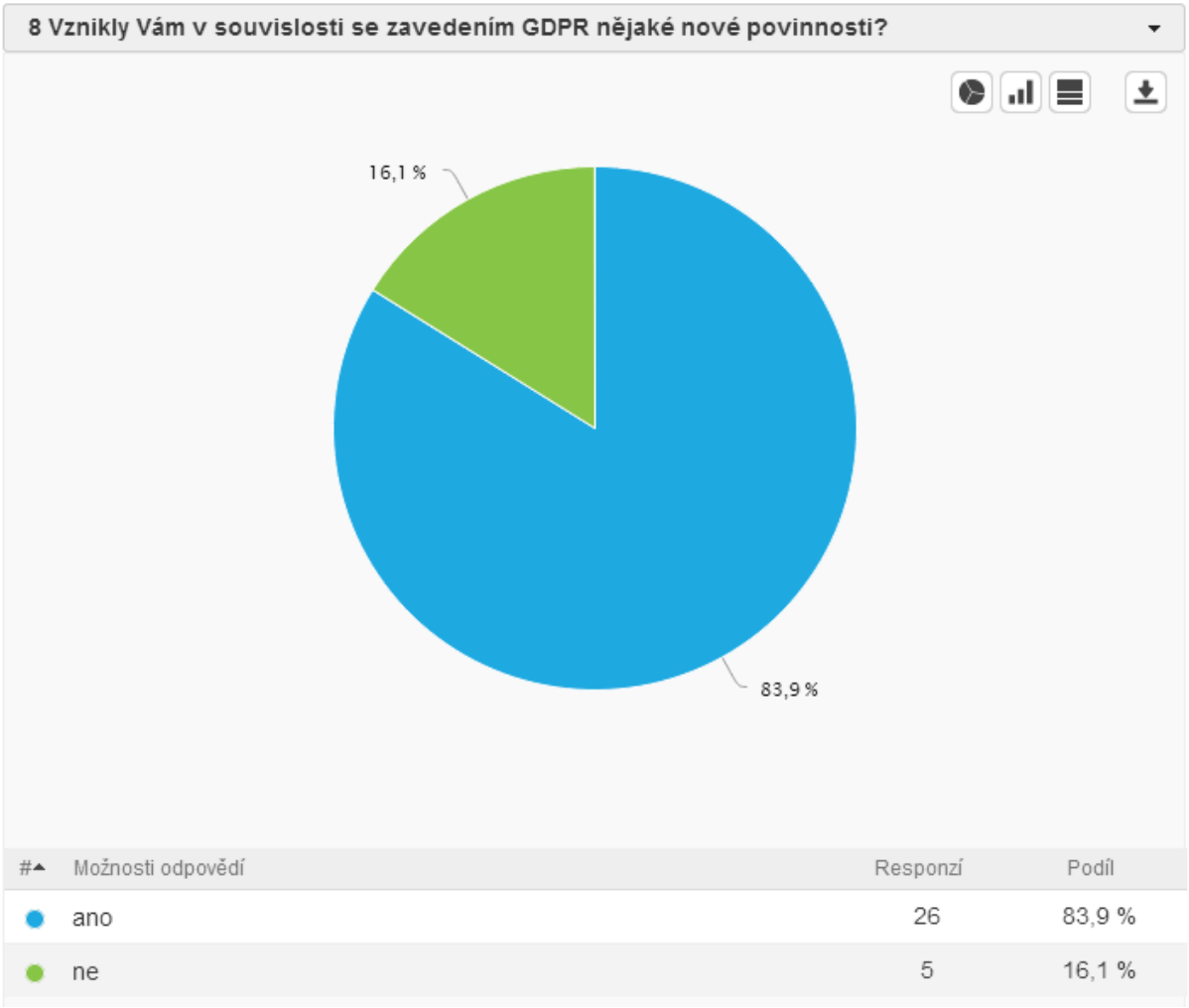
Pouze 6 respondentů z 31 dotázaných v rámci své pracovní náplně zveřejňuje osobní údaje studentů, zaměstnanců či osob v dodavatelsko-odběratelských vztazích a všichni dodržují jejich zabezpečení formou anonymizace nebo pseudonymizace. U ostatních zaměstnanců je tato otázka bezpředmětná.



#	Možnosti odpovědí	Responzí	Podíl
1	V uzamykatelné skříni	0	0 %
2	V uzamykatelné skříni a uzamykatelné kanceláři	26	83,9 %
3	V uzamykatelné místnosti bez dalšího zabezpečení	5	16,1 %
4	Nejsou zabezpečeny	0	0 %

Graf 7: Odpovědi na otázku č. 7

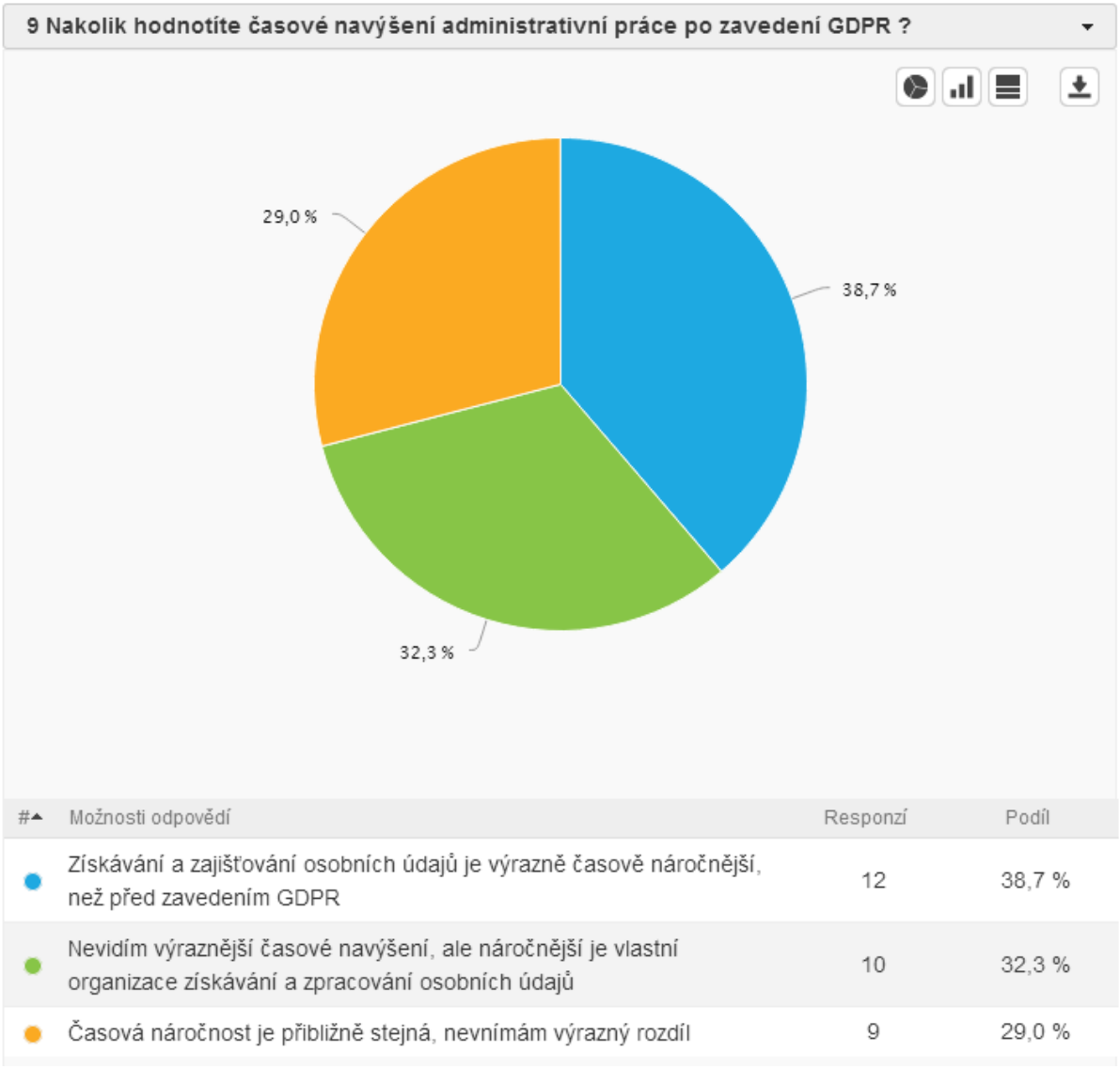
V otázce fyzického zabezpečení bylo zjištěno, že všichni zaměstnanci mají k dispozici uzamykatelnou kancelář a 26 z nich dále disponuje uzamykatelnou skříňkou. 5 zaměstnanců nevyužívá možnosti dvojího zabezpečení.



#	Možnosti odpovědí	Responzí	Podíl
●	ano	26	83,9 %
●	ne	5	16,1 %

Graf 8: Odpovědi na otázku č. 8

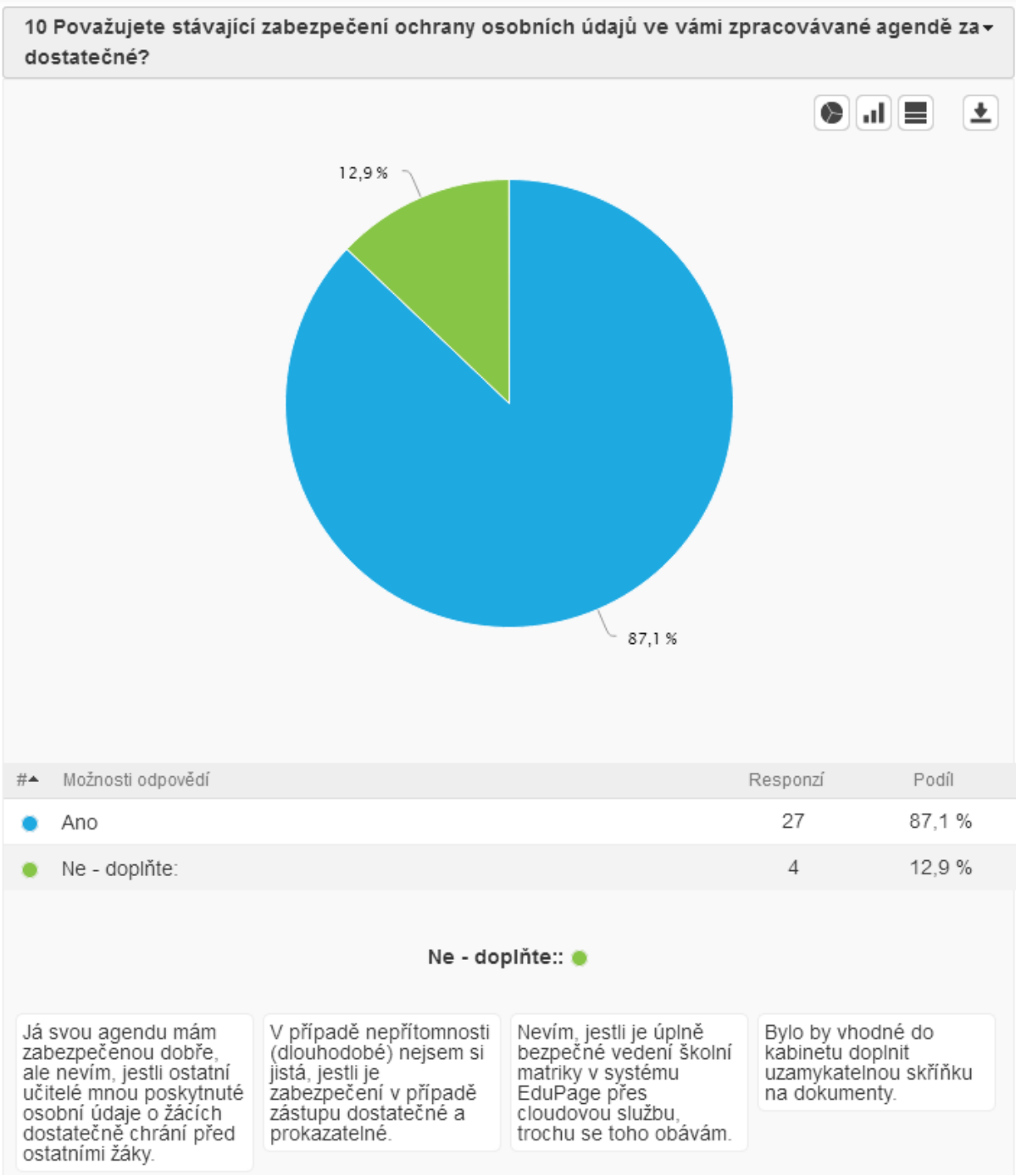
26 respondentů se domnívá, že v souvislosti se zavedením GDPR jim vznikly nové povinnosti. Zbývajících 5 respondentů vznik nových povinností nevnímá.



#	Možnosti odpovědí	Responzí	Podíl
●	Získávání a zajišťování osobních údajů je výrazně časově náročnější, než před zavedením GDPR	12	38,7 %
●	Nevidím výraznější časové navýšení, ale náročnější je vlastní organizace získávání a zpracování osobních údajů	10	32,3 %
●	Časová náročnost je přibližně stejná, nevnímám výrazný rozdíl	9	29,0 %

Graf 9: Odpovědi na otázku č. 9

Co se týče hodnocení z hlediska zvýšení časové náročnosti po zavedení GDPR mají všechny možnosti odpovědí podobné zastoupení, 12 respondentů uvádí výrazné navýšení časové náročnosti, 10 respondentů zmiňuje spíše organizační náročnost a zbývajících 9 respondentů neshledává výrazný rozdíl oproti předchozí situaci.



Graf 10: Odpovědi na otázku č. 10

27 respondentů považuje zabezpečení osobních údajů v rámci své agendy za dostačující. Zbývající 4 respondenti vyjádřili určité obavy z nedostatečného zabezpečení, především v oblasti personálních opatření, tedy selhání lidského faktoru, a informačních opatření, konkrétně byla zmíněna obava z možného kybernetického útoku na školné systém EduPage. Jedním z respondentů zmíněna vhodnost doplnění uzamykatelné skříňky do kabinetu.

10 Shrnutí a vyhodnocení

Za zpracování osobních údajů se podle nařízení GDPR považuje taková činnost s osobními údaji, která vykazuje prvky systematičnosti nebo je prováděna pomocí prostředků výpočetní techniky (automatizované postupy). Osobním údajem je jakákoliv informace, díky které lze identifikovat konkrétní fyzickou osobu (např. rodné číslo, jméno a příjmení), nebo taková informace, na základě které fyzickou osobu sice identifikovat nelze, ale postačí, je-li taková informace přiřazena k již identifikované osobě (např. údaj o mzdě).

Hlavní náplní činnosti Správce je výkon veřejné správy na úseku školství podle zákona č.561/2004 Sb., školského zákona a dalších právních předpisů. V rámci této činnosti dochází k nakládání s osobními údaji několika skupin osob. Primárně se jedná o osobní údaje žáků a zaměstnanců Správce, a to zejména při provádění úkonů v postavení subjektu veřejné správy. S osobními údaji uvedených kategorií subjektů osobních údajů zachází Správce ve značném rozsahu. Mimo uvedené kategorie při své běžné činnosti Správce zachází, a to v menším rozsahu, s osobními údaji dodavatelů služeb, nebo rodinných příslušníků zaměstnanců a žáků.

Pokud se jedná o jednotlivé činnosti zpracování, bylo na základě analýzy situace v organizaci identifikováno několik rozsáhlých činností, při nichž dochází ke zpracování osobních údajů. Jedná se především o tvorbu evidencí žáků (správní rozhodnutí, školní matrika, evidenční listy, třídní knihy apod.), v nichž jsou zaznamenávány důležité informace, které jsou nezbytné pro výkon veřejné správy na úseku školství, dále evidence zaměstnanců, v níž jsou zaznamenávány a uchovávány nejdůležitější informace týkající se pracovně-právní oblasti a také vedení správních evidencí a provádění jednotlivých činností školské veřejné správy. Mimo uvedené základní činnosti dochází ke zpracovávání osobních údajů také v oblasti dodavatelsko-odběratelských vztahů a při provozování internetových stránek.

Při procesech zpracování osobních údajů dochází ke zpracování kategorie OÚ označované jako identifikační osobní údaje jako např. jméno, příjmení, datum narození, adresa trvalého bydliště, kontaktní adresa, rodné číslo, kontaktní údaje apod. Rovněž dochází ke zpracování citlivých osobních údajů, a to ve značném rozsahu, neboť subjektem údajů je z velké části dítě (žák).

Při analýze situace v oblasti ochrany osobních údajů byly využity informace zjištěné jak od ředitelky školy, tak z dotazníkového šetření mezi zaměstnanci, takže se jedná o všestranný

náhled do chodu organizace.

10.1 Zjištěné nedostatky

Na základě analýzy zkoumané organizace bylo zjištěno, že ochrana osobních údajů je zde prováděna v souladu se základními bezpečnostními standardy. Organizace provedla mnohá opatření, aby zajistila soulad ochrany osobních údajů s požadavky stanovenými Nařízením. Přes tuto snahu však nelze říci, že již neexistuje další prostor pro zlepšení, jelikož byly zjištěny občasné dílčí nedostatky. Přehled zjištěných nedostatků a jejich řešení:

- **Opatření fyzické bezpečnosti**

  Zjištěné nedostatky:

  - v některých kancelářích nejsou zajištěny uzamykatelné skříně či boxy k ukládání dokumentů obsahujících osobní informace.

  Řešení:

  - tyto chybějící úložné prostory doplnit a zajistit, aby k dokumentům měl přístup jenom oprávněný zaměstnanec.

- **Opatření informační bezpečnosti**

  Zjištěné nedostatky:

  - nedostatečné zajištění nosičů, na kterých jsou uloženy osobní údaje.

  Řešení:

  - i v této oblasti byl zjištěn stejný nedostatek jako v té předchozí, tedy nejsou dostatečně zajištěny uzamykatelné úložné prostory, kam ukládat mobilní telefony, flash disky, externí hard disky, CD nosiče, digitální fotoaparáty, notebooky. Nutno doplnit.

- **Opatření personální bezpečnosti**

  Zjištěné nedostatky:

  - v oblasti personálních bezpečnostních opatření bylo zjištěno, že osobní údaje při vzájemném zastupování zaměstnanců během výkonu jejich pracovní činnosti nejsou dostatečně zajištěny.

  Řešení:

  - Je potřeba vnitřním předpisem zaměstnavatele vymezit oprávnění jednotlivých

zaměstnanců při zastupování a stanovit přístupová hesla pro jednotlivé osoby v rámci každé agendy.

10.2 Doporučení

Každý Správce osobních údajů má povinnost v rámci procesů zpracování osobních údajů zajistit a nastavit taková technická opatření, která budou s ohledem na závažnost osobních údajů přiměřená pro zajištění odpovídající úrovně důvěrnosti. Organizační opatření pro zabezpečení důvěrnosti osobních údajů se zase týkají především procesů zacházení s osobními údaji zaměstnanci a mají za cíl zabezpečit náležité zpracování. Smyslem je prevence úniku nebo zneužití osobních údajů způsobeného lidským faktorem.

V rámci proaktivního zajištění ochrany osobních údajů, tedy ochrany údajů preventivní (předběžné), nikoli retrospektivní (odstraňování nedostatků až v následku), je třeba systematicky dbát na dodržování veškerých opatření fyzické, personální i informační bezpečnosti.

- **Další doporučení v oblasti opatření fyzické bezpečnosti:**
  - zajistit, aby do místností a skříní měly přístup pouze oprávněné osoby (nesdílet klíče od kanceláří, skříní apod.), v tomto směru instruovat zaměstnance,
  - zabránit vstupu neoprávněných osob do objektu školy (v tomto směru už vedení školy podniklo první kroky, jelikož zařadilo nový bezpečnostní systém jako prioritu pro příští období).

- **Další doporučení v oblasti opatření informační bezpečnosti:**
  - vždy používat bezpečné heslo (mělo by obsahovat alespoň 8 znaků, velká i malá písmena, číslice, případně speciální znaky),
  - heslo v pravidelných intervalech měnit,
  - v případě podezření, že se k heslu dostala neautorizovaná osoba, okamžitě ho změnit,
  - nenechávat napsané heslo na nějakém viditelném místě,
  - nikdy nenechávat bez dohledu počítač, na kterém je uživatel přihlášen pod svým jménem a heslem, při odchodu se vždy odhlásit,
  - v emailové komunikaci dávat pozor na odeslání špatnému adresátovi a odpovědi na nevyžádanou poštu a otevírání podezřelých nevyžádaných

příloh,

- co se externích přenosných úložišť týče, je třeba dbát na jejich bezpečnost a nepoužívat zařízení bez zašifrování a s podezřením na zavirování,
- přenosné nosiče dat ukládat do uzamykatelných prostor a nenechávat je volně přístupné bez dozoru na stole apod.,
- u mobilních telefonů využívaných zaměstnanci pro přístup do školního systému EduPage nastavit funkci zamykání obrazovky a nainstalovat zde aktuální antivirový program,
- dostatečně zabezpečit systém EduPage proti případným kybernetickým útokům.

- **Další doporučení v oblasti opatření personální bezpečnosti:**
  - průběžně proškolovat personál ohledně dodržování bezpečnostních opatření,
  - zajistit realizaci práv subjektů osobních údajů na přístup k osobním údajům, opravu, výmaz, přenositelnost, omezení zpracování nebo podání stížnosti,
  - řádně dodržovat transparentnost a informační povinnost vůči subjektům osobních údajů, nejlépe v písemné či elektronické podobě, a to z důvodu jasného prokázání splnění této povinnosti,
  - provádět namátkové kontroly zaměstnanců ohledně dodržování instrukcí zaměstnavatele.

ZÁVĚR

Cílem této bakalářské práce bylo popsat hlavní změny v povinnostech zaměstnavatelů v návaznosti na vstoupení v účinnost Obecného nařízení Evropského parlamentu a Rady o ochraně osobních údajů č. 2016/679 Obecného nařízení o ochraně osobních údajů, se zaměřením zvláště na povinnosti nově vyplývající. Tato práce je rozdělena na dvě části: teoretickou a praktickou. V teoretické části jsem uvedla obecné informace o GDPR, jeho působnost, hlavní znaky a také jsem objasnila základní pojmy a zásady. Praktická část práce byla zaměřena na průzkum v organizaci Gymnázium Šternberk ohledně konkrétních dopadů implementace Nařízení.

V úvodu praktické části jsem blíže charakterizovala zkoumanou organizaci – Gymnázium Šternberk. S ohledem na skutečnost, že se jedná o školskou organizaci, je zde zpracováváno opravdu velké množství osobních údajů různých skupin subjektů, zejména žáků, jejich zákonných zástupců a zaměstnanců. Z tohoto důvodu je zde otázka dodržení všech povinností vyplývajících z Nařízení velmi aktuální.

Nejprve jsem provedla vstupní šetření formou rozhovoru s ředitelkou školy, na základě kterého jsem zjistila, jaké osobní údaje jsou zde zpracovávány, kým a jakým způsobem. Dalším důležitým zjištěním byly informace o opatřeních, která byla v dané organizaci učiněna po zavedení GDPR, a to opatření v oblasti fyzické, informační a personální bezpečnosti ochrany osobních údajů.

Dalším krokem analýzy bylo dotazníkové šetření, v jehož rámci byli osloveni všichni zaměstnanci školy, kteří při své pracovní činnosti osobní údaje různých subjektů zpracovávají, což jsou všichni pedagogičtí pracovníci a dále pracovnice ekonomického úseku. Otázky v dotazníku byly zaměřeny na zjištění pracovních pozic zaměstnanců, obsah a rozsah zpracovávaných osobních údajů v rámci jednotlivých agend v organizaci, používání technických prostředků, způsob zabezpečení a hodnocení navýšení pracovních povinností v souvislosti se zavedením GDPR. Tohoto dotazníkového šetření se zúčastnilo 88,57% oslovených zaměstnanců.

Výstupem této analýzy bylo zhodnocení situace ochrany osobních údajů v organizaci, popis zjištěných nedostatků s návrhem jejich řešení a další doporučení preventivních opatření v oblasti ochrany osobních údajů.

POUŽITÁ LITERATURA A INTERNETOVÉ ZDROJE

Důvodová zpráva k Zákonu č. 110/2019, Sb. o zpracování osobních údajů. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=138&CT1=0.

E15.cz: Šéfka Úřadu pro ochranu osobních údajů: Vysokými pokutami chceme firmy odrazovat, ne likvidovat [online]. Změněno 25. 5. 2018. Dostupné z: https://www.e15.cz/rozhovory/sefka-uradu-pro-ochranu-osobnich-udaju-vysokymi-pokutami-chceme-firmy-odrazovat-ne-likvidovat-1334926.

Epravo.cz: Nový zákon o zpracování/ osobních údajů [online]. Změněno dne 30. 5. 2019. Dostupné z: https://www.epravo.cz/top/clanky/novy-zakon-o-zpracovani-osobnich-udaju-109312.html

Evropská komise: Zásady GDPR [online]. [cit. 3. 4. 2019]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_cs

Evropský sbor pro ochranu osobních údajů: Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679 17 [online]. [cit. 3. 4. 2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31886

GDPR.cz: Adaptační zákon prošel sněmovnou [online]. Změněno 2. 1. 2019. Dostupné z: https://www.gdpr.cz/blog/adaptacni-zakon-prosel-snemovnou/

GDPR.cz: Přenositelnost [online]. Změněno 31. 1. 2018. Dostupné z: https://www.gdpr.cz/blog/prenositelnost/

GDPR.cz: Sankce [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/

Gymnázium Šternberk: Výroční zpráva o činnosti školy ve školním roce 2017/2018. Dostupné online https://cloud5.edupage.org/cloud/Vyrocka_pracovni_rev3.pdf?z%3AaFcNlqO7mPSq1wSnAr3ixpyDP%2FOdqZ5RHQNk9df9nm8vhQ3XFcxSuH1php90MV3%2B

Gymst.com: Historie [online]. [cit. 12. 6. 2019]. Dostupné z: http://80.gymst.com/index2.html

KOHÚTOVÁ, Zuzana a Pavel KYSELÁK. *GDPR pro účetní a mzdové účetní*. Praha: Svaz účetních České republiky, 2018. Metodické aktuality. 64 stran. ISBN 978-80-87367-86-5.

KOLEKTIV AUTORŮ. *GDPR 2018 v praxi*. Praha: Verlag Dashöfer, nakladatelství, s.r.o., 2018. 262 stran.

Ministerstvo vnitra České republiky. Orientace v GDPR [online]. [cit. 3. 4. 2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Úř. věst. L 119 4.5.2016.

Podnikatel.cz. Další zpoždění, Senát adaptační zákon k GDPR vrátil. Víme, co nového přináší [online]. Změněno dne 1. 2. 2019. Dostupné z: https://www.podnikatel.cz/clanky/adaptacni-zakon-k-gdpr-upresnuje-pokuty-a-vekove-omezeni-pro-udeleni-souhlasu/

Šandera, David: *Dopady obecného nařízení o ochraně osobních údajů na firemní procesy.* Diplomová práce, VŠT v Praze, 2017.

Uoou.cz: Adaptační legislativa k GDPR vstoupila v účinnost [online]. Změněno dne 25. 4. 2019. Dostupné z: https://www.uoou.cz/adaptacni-legislativa-k-nbsp-gdpr-vstoupila-v-nbsp-ucinnost/d-33656

Uoou.cz: Práva subjektu údajů [online]. Změněno 25. 4. 2019. Dostupné z https://www.uoou.cz/6-prava-subjektu-udaju/d-27276

Uoou.cz: Sankce, pokuty [online]. Změněno 25. 4. 2019. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287/p1=4744.

Uoou.cz: Základní příručka k GDPR [online]. [cit. 25. 4. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2075

Uoou.cz: Zaměstnavatel jako správce osobních údajů [online]. Změněno 13. 12. 2013. Dostupné z: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171/p1=3938

Vnitřní organizační řád Gymnázia Šternberk, platnost od 1. 2. 2013

Voigt, Paul & von dem Bussche, Axel. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. 385 stran. ISBN 978-3-319-57959-7.

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

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

Zákon č. 418/2011, Sb., o trestní odpovědnosti právnických osob a řízení proti nim

Zákon č. 40/2009, Sb. trestní zákoník

Zřizovací listina Gymnázia Šternberk v úplném znění ze dne 19. 12. 2016

ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 344 stran. ISBN 978-80-7554-152-9.

Seznam použitých zkratek

BOZP	Bezpečnost a ochrana zdraví při práci
ČŠI	Česká školní inspekce
DIČ	Daňové identifikační číslo
EU	Evropská Unie
GDPR	Obecné nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/45/ES
IČ	Identifikační číslo
ÚOOÚ	Úřad pro ochranu osobních údajů

Seznam tabulek

Seznam grafů

Seznam obrázků

Seznam příloh

Příloha 1: Prohlášení o ochraně osobních údajů

PROHLÁŠENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

*podle ustanovení článku 12, 13 a 14 Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „**GDPR**“)*

Jestliže žák navštěvuje naši školu – Gymnázium, Šternberk, Horní náměstí 5 (dále jen „škola“ nebo „správce“), stáváme se správcem osobních údajů. V takovém případě máme povinnost sdělit všem subjektům osobních údajů určité informace o zpracovatelských činnostech. Účelem zpracování osobních údajů studenta je především řádné poskytování vzdělání podle příslušných právních předpisů a realizace dalších úkonů, spojených s činností školy viz dále.

Z níže uvedených zásad o ochraně osobních údajů, zjistíte veškeré relevantní informace tykající se ochrany Vašich osobních údajů. Především pak získáte informace, jaké osobní údaje jsou zpracovávány, jaký je účel jejich zpracování, způsob zpracování osobních údajů a délku uchovávání osobních údajů studentů naší školy. Uvedené informace jsou důležité, proto doufáme, že si najdete čas a pečlivě si vše přečtete.

V případě jakýchkoliv nejasností nebo zájmu o bližší informace nás můžete navštívit na adrese Horní náměstí 5 nebo nás kontaktovat prostřednictvím e-mailu podatelna@gymst.cz.

Dále bychom vám rádi oznámili, že pro oblast ochrany osobních údajů jsme v naší škole jmenovali pověřence pro ochranu osobních údajů (dále jen „pověřenec“). Pověřencem může být v oblasti ochrany osobních údajů jen odborně znalá osoba, která má například za úkol dohlížet na řádné zacházení s osobními údaji, poradit správci údajů, jak nejlépe dodržovat řádné principy pro ochranu osobních údajů a v neposlední řadě se na něj také můžete obracet i vy se svými dotazy nebo žádostmi. V naší škole vykonává funkci pověřence Schola Servis GDPR, s.r.o., se sídlem Palackého 150/8, Prostějov, IČ: 04223748 a kontaktovat jej můžete na mob.: 732 464 854, 732 657 386, 733 281 378, email:poverenec@gdprdoskol.cz

V prohlášení o ochraně osobních údajů je například vysvětleno:

- Jaké informace (osobní údaje) shromažďujeme, z jakého důvodu a na základě jakého právního titulu
- Jak tyto informace využíváme
- Po jakou dobu budeme s těmito informacemi nakládat
- Kdo může do osobních údajů nahlížet (tzv. příjemci osobních údajů)
- Jaká mají děti a jejich zákonní zástupci práva vůči správci osobních údajů

Snažíme se, co možná nejvyšší přehlednost a srozumitelnost tohoto dokumentu. Pokud se však stane, že některé námi užívané výrazy jsou pro vás neznámé, nebo nesrozumitelné neboť se jedná o právní pojmy (jako například zpracovatel osobních údajů, pseudonymizace apod.), pak neváhejte a obraťte se na nás nebo na pověřence. Rádi vám podrobnosti objasníme.

Informace, se kterými nakládáme a doba jejich zpracování

<u>Správní řízení</u>

Přihlášku ke studiu na střední škole podává uchazeč řediteli střední školy. Na základě přihlášky ke vzdělávání se uchazeč zúčastní přijímacího řízení. Ředitel školy na základě zhodnocení splnění či nesplnění kritérií přijímacího řízení vydá rozhodnutí o přijetí/nepřijetí ke studiu. Celý tento proces je tzv. správním řízením, kdy ředitel školy (jako správní orgán) zde rozhoduje o právech a povinnostech jmenovitě určené osoby.[58] Abychom mohli takové správní řízení konat, potřebujeme znát následující základní identifikační nebo popisné osobní údaje studenta:

- Student: jméno a příjmení, datum narození, případně rodné číslo (u oborů s maturitní zkouškou), státní občanství, místo trvalého pobytu případně adresa pro doručování
    - Další osobní údaje, které můžou být zpracovávány jsou: závěr o zdravotní způsobilosti ke vzdělávání na základě lékařského posudku, informace o schopnostech, vědomostech, zájmech uchazeče/žáka, stupeň podpůrných opatření, obor vzdělání, o který má zájem přijatý uchazeč (na základě vyhlášeného rozhodnutí o přijetí), obor vzdělávání, forma vzdělávání - v případě nezbytných informací o zdravotním stavu se jedná o zvláštní kategorii údajů – tzv. citlivé údaje.
- Zákonný zástupce: jméno a příjmení, adresa trvalého pobytu nebo adresa pro doručování písemností, ID datové schránky (pokud byla zpřístupněna), telefonní číslo nebo e-mail.

Tyto osobní údaje zpracováváme za účelem plnění právní povinnosti, a to vedení správního řízení (řízení o rozhodnutí o přijetí ke vzdělávání na střední škole). Právním titulem pro zacházení s těmito informacemi je podle článku 6 odst. 1 písm. c) GDPR[59] plnění právní povinnosti, a to podle ust. § 60a, § 60d, §60e, § 183 zákona č. 561/2004 Sb., školský zákon a dále §1 odst. 2 vyhl. č. 353/2016 Sb., zákon č. 373/ 2011 Sb., vyhl. č. 98/ 2012 Sb., § 16 a násl. školského zákona a vyhl. č. 27/2016 Sb., § 37 odst. 2 zákona č. 500/2004 Sb., správní řád, jakož i prováděcí právní předpisy k výše uvedeným zákonům.

Zpracování výše uvedených osobních údajů probíhá také na základě právního titulu podle článku 6 odst. 1 písm. e) GDPR výkon veřejné moci, kterým je správce pověřen. Výkon veřejné správy ředitelů škol všech zřizovatelů při přijímání ke vzdělávání ve střední škole je podle § 165 odst. 2 školského zákona rozhodováním podle správního řádu.

Za účelem vedení správního řízení osobní údaje shromažďujeme (archivujeme) po dobu, která je stanovená ve spisovém a skartačním plánu školy. V případě žádostí o přijetí ke vzdělávání na střední škole a rozhodnutí o přijetí se jedná o dobu 10 let, u zápisových lístků je doba stanovena taktéž 10 let.

Řízení o přijetí k vzdělávání není jediným správním řízením, které se při vzdělávání studentů může konat. Další řízení mohou být např. řízení o ukončení středního vzdělávání bez výučního listu a bez maturitního osvědčení (§ 28 školského zákona) dle § 1 odst. 2 a příloha č. 3 vyhl. č. 3/2015 Sb., řízení o ukončení středního vzdělávání s výučním listem (§ 28 školského zákona, § 1 odst. 2 a příloha č. 4 vyhlášky č.3/2015Sb., řízení o ukončení středního vzdělávání s maturitní zkouškou (§ 81 odst. 1 školského zákona, § 4 a Příloha č. 1 vyhlášky č. 177/2009 Sb.), osvědčení o jednotlivé zkoušce, která odpovídá zkoušce SČ MZ (§ 48 odst. 7 a Příloha č. 5 vyhlášky č. 177/2009 Sb.), osvědčení o jednotlivé zkoušce, která odpovídá zkoušce PČ MZ (§ 49 odst. 7 a Příloha č. 6 vyhlášky č. 177/2009 Sb), řízení o vydání vysvědčení o maturitní zkoušce (§ 28 odst. 7 školského zákona, § 81 odst. 4 školského zákona,

[58] viz § 9 zákona č. 500/2004 Sb., správní řád.

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

§ 1 odst. 2 a příloha č. 5 vyhlášky č. 3/2015 Sb.), žádosti o vydání duplikátu závěrečného, maturitního vysvědčení, vysvědčení o absolutoriu (§ 28, a § 164 odst. 1 školského zákona, § 4 vyhlášky č. 3/2015 Sb. a zákona č. 106/1999 Sb., zákon o svobodném přístupu k informacím). U správních rozhodnutí výše uvedených je doba skartace stanovena na 50 let, pokud nejde o archiválie podle bodu 16 přílohy č. 2 zákona č. 499/2004 Sb. Mohou zde probíhat i další správní řízení v souladu se správním řádem.

Matrika studentů a ostatní dokumentace škol

Školský zákon ukládá všem školám povinnost, aby vedly určitou dokumentaci o své činnosti. Mezi povinnou dokumentaci patří i vedení tzv. evidence studentů podle § 28 odst. 1 písm. b) školského zákona. Jedná se o tzv. školní matriku. Její náležitosti jsou stanoveny v § 28 odst. 2 školského zákona. Ve školní matrice proto musíme vést následující osobní údaje:

- Studenta: jméno a příjmení, rodné číslo, datum narození, státní občanství, místo narození a místo trvalého pobytu, popřípadě místo pobytu na území České republiky podle druhu pobytu cizince nebo místo pobytu v zahraničí nepobývá-li dítě, žák nebo student na území ČR, údaje o předchozím vzdělávání vč. dosaženého stupně vzdělání, obor, formu a délku vzdělávání jde-li o střední a vyšší odbornou školu, datum zahájení vzdělávání ve škole, údaje o průběhu a výsledcích vzdělávání ve škole, vyučovací jazyk, údaje o znevýhodnění uvedeném v § 16 školského zákona, údaje o mimořádném nadání, údaje o poskytovaných podpůrných opatřeních, závěry vyšetření uvedených v doporučení školského poradenského zařízení, údaje o zdravotní způsobilosti ke vzdělávání a o zdravotních obtížích, které by mohly mít vliv na průběh vzdělávání, datum ukončení vzdělávání ve škole, údaje o zkoušce, jíž bylo vzdělávání ve střední nebo vyšší odborné škole ukončeno
    - zde se jedná převážně o základní identifikační nebo popisné osobní údaje, nicméně v určitém rozsahu se zpracovávají i informace o zdravotním stavu, které jsou považovány za zvláštní kategorii osobních údajů – tzv. citlivé údaje
- Zákonného zástupce: jméno a příjmení zákonného zástupce, místo trvalého pobytu nebo bydliště, pokud nemá na území České republiky místo trvalého pobytu, a adresu pro doručování písemností, telefonické spojení
    - zde se jedná o základní identifikační nebo popisné osobní údaje
- Abychom mohli se zákonnými zástupci efektivně a rychle komunikovat, mohou nám zákonní zástupci dát dobrovolně svůj e-mail. Takový osobní údaj je poté zpracováván na základě oprávněného zájmu správce osobních údajů podle článku 6 odst. 1 písm. f) GDPR, a to za účelem efektivní komunikace.

Tyto osobní údaje zpracováváme za účelem plnění právní povinnosti – vedení evidence studentů – vedení školní matriky. Ve školní matrice jsou tak osobní údaje zpracovávány na základě plnění právní povinnosti, která naší škole vyplývá ze školského zákona. Zpracování takovýchto údajů je proto v souladu s článkem 6 odst. 1 písm. c) GDPR. Školní matrika se uchovává po dobu, kterou stanovuje zákon o archivnictví a spisové službě[60], a to po dobu 10 let, ledaže se jedná archiválie podle bodu 16 přílohy č. 2 zákona o archivnictví a spisové službě, které se vždy povinně předkládají státnímu archivu k výběru za archiválie.

Školní matriky nejsou jediným dokumentem, který má škola povinnost vypracovávat. Mezi další povinné dokumenty, kde se objevují osobní údaje studentů, jsou např. třídní knihy a třídní výkazy studentů, katalogové listy, zápisy z porad, knihy úrazů aj. Účelem zpracování osobních údajů v takových dokumentech je poté řádné plnění pedagogické činnosti a plnění právních povinností při poskytování vzdělávání. Doba uchování těchto dokumentů je uvedena ve spisovém a skartačním řádu

[60] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

školy a různí se podle typu dokumentu. Evidence záznamů v třídní knize jsou ukládány po dobu 10 let, naopak žádosti o přestup, výsledky orientačního testování na přítomnost OPL nebo evidence některých úrazů jsou ukládány po dobu 5 let a zápisy z pedagogických rad 10 let. Takové zpracování je opět prováděno na základě plnění právních povinností, a tedy v souladu s článkem 6 odst. 1 písm. c) GDPR.

Stravování

Abychom mohli studentům řádně poskytovat stravovací služby, pak i za tímto účelem musíme zpracovávat informace, které jsou uváděny nejčastěji v přihláškách ke stravování. Jedná se o následující osobní údaje:

- Studentů: jméno a příjmení, datum narození nebo rodné číslo, státní občanství, místo trvalého pobytu nebo adresa bydliště (kontaktní adresa), školní rok, třída, číslo bankovního účtu, datum zahájení a ukončení stravovacích služeb, údaje o zdravotních obtížích, které by mohly mít vliv na poskytované služby (např. alergie na lepek)
    - jedná se převážně o základní identifikační nebo popisné osobní údaje, nicméně informace o zdravotních obtížích jsou informace o zdravotním stavu, které jsou považovány za zvláštní kategorii osobních údajů – tzv. citlivé údaje
- Zákonných zástupců: jméno a příjmení, adresa trvalého pobytu nebo bydliště (kontaktní adresa), telefonické spojení nebo email, číslo bankovního účtu

Poskytování stravovacích služeb je uskutečňováno na základě přihlášky ke stravování. Přihláška tak zakládá určitý (právní) vztah, kdy má provozovatel stravovacího zařízení povinnost poskytnout službu a na druhé straně příjemce takové služby má jiné závazky, typicky povinnost uhradit cenu takové služby. Přihláška ke stravování by se tak dala považovat za jakousi smlouvu. V takovém případě se zpracování výše uvedených osobních údajů za účelem poskytování stravovacích služeb děje na základě plnění smluvního vztahu podle článku 6 odst. 1 písm. b) GDPR.

Přihlášení do projektu ERASMUS

Může se také stát, že naše škola bude partnerem v rámci projektu ERASMUS. V rámci výměnných pobytů studentů v rámci rozšíření vzdělání a jazykových dovedností dochází ke zpracovávání osobních údajů. Hostitelské školy v zahraničí zajišťuje právě projekt ERASMUS. V rámci přihlášení do tohoto projektu správce na základě řádně uděleného souhlasu může zpracovávat následující osobní údaje:

- Jméno a příjmení studenta, datum narození, rodné číslo, bydliště, číslo OP, telefon, e-mail, jméno a příjmení zákonného zástupce, adresa trvalého pobytu.

S údaji pracují pověření pracovníci zajišťující projekt Erasmus.

Prezentace školy a bezpečnost

Pro účely prezentace školy využíváme internetové stránky (www.gymst.cz, www.gymst.com, www.gymst.eu), naší facebookovou stránku (facebook školy) nebo zveřejňujeme některé důležité zprávy v běžných médiích (např. místní tisk nebo regionální TV). Může se tedy stát, že za účelem informování veřejnosti o dění v naší škole a pro prezentaci školy zveřejníme jméno a příjmení studenta a případně i fotografii, audio a videozáznam nebo výtvarné dílo. Nemusíte se ale bát, k takovému zveřejnění vyžadujeme souhlas se zpracováním osobních údajů.

Rádi bychom vás upozornili, že pro některé zveřejňování fotografií nebo videozáznamů není souhlas se zpracováním údajů potřebný. Tak je tomu v případě, kdy na dané fotografii nebo videozáznamu není konkrétní osoba zcela identifikovatelná. Pokud i přesto budete žádat, aby taková fotografie nebo videozáznam nebyl zveřejněn, pak to chápeme a můžete se s žádostí o smazání obrátit na výše uvedené kontakty školy nebo pověřence.

Nejen ochrana soukromí studentů školy je pro nás důležitá. Dbáme zároveň ochrany jejich zdraví, bezpečí a majetku. Proto mohou být v naší škole instalovány kamerové systémy, které však snímají pouze nezbytné prostory pro zajištění bezpečnosti. Archiv záznamů je v souladu s doporučeními Úřadu pro ochranu osobních údajů ukládán pouze po dobu nejdéle několika dní.

Hospodářská činnost a účetnictví

Hlavní činností naší školy je poskytování vzdělávání. Abychom mohli plnit naší hlavní činnost řádně a svědomitě, potřebujeme zajistit běžný chod školy – např. zajištění účetnictví, provoz telefonů, IT sítě, ale i třeba běžná údržba budovy. Za tímto účelem uzavíráme různé soukromoprávní smlouvy s dodavateli služeb. I v těchto smlouvách se objevují osobní údaje smluvních partnerů.

- nejčastěji se jedná o následující osobní údaje: jméno a příjmení, identifikační číslo podnikatele, adresa provozovny nebo sídla, adresa trvalého pobytu nebo bydliště (kontaktní adresa), daňové identifikační číslo, e-mail a telefon.

S těmito osobními údaji zacházíme převážně za účely plnění uzavřené smlouvy, tj. podle článku 6 odst. 1 písm. b) GDPR, ale zároveň i pro plnění smluvních povinností, tj. podle článku 6 odst. 1 písm. c) GDPR. Plnění smluvních povinností nastává typicky v případě, kdy na základě uzavřené smlouvy musíme evidovat v rámci účetnictví faktury nebo jiné daňové doklady podle zákona č. 563/1991 Sb., o účetnictví. Smlouvy se uchovávají nejdéle po dobu 10 let, protože mohou být předmětem kontroly ze strany zřizovatele a faktury po dobu 5 let.

Poučení o právech subjektů osobních údajů

Každý subjekt osobních údajů má následující práva[61]:

- požadovat omezení zpracování osobních údajů,
- požadovat vysvětlení ohledně zpracování osobních údajů,
- požadovat informaci, jaké osobní údaje jsou na základě souhlasu zpracovávány,
- vzít souhlas se zpracováním údajů kdykoliv zpět,
- vyžádat si přístup k údajům a nechat je aktualizovat, opravit nebo doplnit,
- požadovat výmaz osobních údajů,
- v případě pochybností o dodržování pravidel souvisejících se zpracováním osobních údajů se obrátit na správce nebo se stížností na Úřad pro ochranu osobních údajů (www.uoou.cz)

Příjemci osobních údajů

Svěřeným osobním údajům věnujeme velikou opatrnost. To zahrnuje především starat se o to, aby k nim měly přístup jen osoby, které jsou oprávněny s takovými informacemi nakládat. Při výkonu naší činnosti se může stát, že k osobním údajům bude mít přístup i další osoba. Tak je tomu typicky v případech orgánu veřejné moci, které provádí kontrolní činnost, orgánů zřizovatele školy nebo osob, které zajišťují pro školu služby nebo jiné činnosti (např. pořadatel školních soutěží, organizátor akce jako je zájezd, poskytovatel projektu ERASMUS, smluvní strana zabezpečující výkon odborné praxe apod.). Příjemci osobních údajů získávají pouze jen ty osobní údaje, které nezbytně potřebují pro zajištění a výkon činnosti vůči škole.

[61] Práva jsou uvedená v článcích 12 až 23 GDPR.

Zabezpečení osobních údajů

Víme, že ochrana soukromí studentů, ale i ostatních kategorií subjektů osobních údajů je důležitou součástí naší činnosti a nepodceňujeme ji. Proto se vždy snažíme zajistit dostatečná opatření, abychom zpracovávaným informacím dopřály odpovídající úroveň důvěrnosti. Pro řádné dodržování ochrany osobních údajů proto využíváme například následující bezpečnostní prvky:

- zaměstnanci školy jsou vázáni mlčenlivostí o skutečnostech, o nichž se dozvěděli při výkonu své práce
- osobní údaje jsou ukládány do uzamykatelných prostorů, kam má přístup pouze omezený počet zaměstnanců školy.
- v případě uchovávání osobních údajů v digitálním prostředí jsou výpočetní prostředky náležitě zabezpečeny jak fyzicky (proti odcizení nebo zničení), tak i programově (proti škodlivým softwarům, nastavením elektronického zabezpečení přístupu jen oprávněným osobám nebo v neposlední řadě také využíváním bezpečných komunikačních kanálů, které využívají prvky šifrování)
- pokud předáváme osobní údaje některým příjemcům (viz výše), vždy se ujišťujeme
    - že se jedná o osoby, které jsou oprávněny s údaji nakládat
    - že nezískávají ty osobní údaje, které nezbytně nepotřebují pro výkon své činnosti
    - že taková osoba s osobními údaji zachází s náležitou péčí a opatrností
    - že příjemce bude dodržovat stejnou mlčenlivost, jakou jsou vázáni zaměstnanci školy
- při zveřejňování výsledků z přijímacího řízení využíváme tzv. pseudonymizaci, kdy výsledky dětí nejsou zveřejňovány pod jejich jménem, ale pod určitým identifikátorem (např. číslo přihlášky k vzdělávání)
- k osobním údajům mají v rámci organizace přístup jen ti zaměstnanci, kteří jsou oprávněni s osobními údaji nakládat
- zabezpečení údajů je průběžně kontrolováno a aktualizováno s ohledem na způsoby jakým se s osobními údaji zachází

Závěr

V naší škole se snažíme zacházet jen těmi osobními údaji, které nezbytně potřebujeme pro výkon svěřené činnosti, tj. poskytování vzdělávání. Ve většině případů s informacemi zacházíme proto, že plníme určitou zákonnou povinnost – v této oblasti jsou stěžejní zejm. předpisy upravující školství. Dalšími právními tituly pro zacházení s osobními údaji je zpracování nezbytné pro plnění smlouvy nebo pro oprávněné zájmy správce. Těchto osobních údajů však zpracováváme malý rozsah. Ve výjimečných případech se může stát, že pro určité zpracování nebo pro určité osobní údaje si musíme vyžádat souhlas se zpracováním. Takový souhlas máte právo například odvolat.

V každém případě s osobními údaji zacházíme jen na nezbytně nutnou dobu, kterou nám nejčastěji ukládá některý právní předpis (typicky zákon o archivnictví a spisové službě, zákon o účetnictví atd.) nebo doba plyne z deklarovaného účelu, za jakým jsou údaje zpracovávány.

Soukromí všech subjektů osobních údajů bereme vážně. Proto se staráme o to, aby veškeré informace byly ukládány na bezpečném místě a aby k nim měly přístup jen ty osoby, které jsou oprávněny s informacemi nakládat. Když předáváme osobní údaje příjemcům, pak je to jen pro výkon činností orgánů veřejné moci (zejm. provádění kontrol a inspekcí) nebo pro subjekty zajišťující služby nebo činnosti, které souvisí se vzděláváním. Vždy však dbáme na to, aby takové předání trvalo jen omezenou dobu, aby příjemce dodržoval stejné standardy ochrany osobních údajů jako škola a v neposlední řadě, aby zacházel pouze s osobními údaji, které opravdu nezbytně potřebuje.

Transparentní zacházení s informacemi je v této oblasti důležitá, proto máte-li nějaké dotazy, napište nám třeba na náš mail podatelna@gymst.cz nebo využijte výše uvedených kontaktů.

Příloha 2: Zásady mlčenlivosti pro oblast osobních údajů

ZÁSADY MLČENLIVOSTI
PRO OBLAST OCHRANY OSOBNÍCH ÚDAJŮ

poučení o mlčenlivosti zaměstnanců

V souvislosti s účinností nového právního předpisu pro oblast ochrany osobních údajů – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o Zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „GDPR"), je nezbytné upravit základní zásady při zacházení s osobními údaji, a poučit o nich zaměstnance, a to následovně:

1) Základní principy, pravidla a povinnosti při zacházení s osobními údaji jsou zpracovány ve Směrnici k o ochraně osobních údajů (dále jen „Směrnice") a každý zaměstnanec řádně dodržuje Směrnici.

2) Každý zaměstnanec je vázán přísnou mlčenlivostí o všech skutečnostech, o nichž se v rámci výkonu své práce dozvěděl vč. veškerých informací týkajících se zpracovávání osobních údajů.

3) Zaměstnanec pověřený spisovou službou dbá na zajištění důvěrnosti osobních údajů uložených ve spisovně školy – zajistí, aby prostor spisovny byl při opouštění místnosti vždy řádně uzamčen a přístupové klíče byly pouze u oprávněné osoby.

4) Každý zaměstnanec v rámci výkonu svého zaměstnání dbá přísných pravidel při zacházení s osobními údaji, zejména:

a. zachovává mlčenlivost o veškerých skutečnostech souvisejících s osobními údaji, s nimiž nakládá v rámci výkonu svého pracovního zařazení (zejm. dbá o ochranu následujících dokumentů – třídní výkazy, třídní knihy, papírové výkazy školní matriky, doporučení z ŠPZ, plány IVP apod.),

b. nesděluje (ani jiným způsobem nezpřístupňuje) svěřené osobní údaje osobám, které nejsou oprávněny k takovým informacím přistupovat (k osobním údajům dětí může přistupovat jen jejich zákonný zástupce),

c. chrání osobní údaje Správce před zneužitím, zničením, neoprávněným pozměněním apod. – např. ukládáním písemných dokumentů do uzamykatelné skříně, uchováváním

elektronických údajů v PC, které jsou přístupné jen po zadání hesla a řádným odhlašováním z využívaných elektronických služeb, nesděluje své heslo ostatním zaměstnancům,

d. shromažďuje v souladu se záznamy o činnostech zpracování pouze nezbytné osobní údaje,

e. osobní údaje ukládá pouze na bezpečných místech, která jsou zabezpečena před neoprávněným přístupem (prostředky manuálního zpracování fyzicky uzamčeny, prostředky automatizovaného zpracování chráněny digitálními prvky – hesla, šifrování),

f. dokumenty obsahující osobní údaje vyřazuje v souladu se spisovým a skartačním řádem školy.

5) Zdravotní dokumentace s citlivými osobními údaji musí být vždy ukládána do uzamykatelných skříní. V případě zdravotních údajů zpracovávaných automatizovaně (v PC), využívat jen PC, které je chráněno heslem, a využívat jen zabezpečený software.

6) Mlčenlivost se vztahuje i na osobní údaje zaměstnanců vedených zaměstnavatelem pro personální a platové účely.

7) Každý zaměstnanec bez zbytečného odkladu ohlašuje zaměstnavateli veškeré skutečnosti, které se týkají změny jeho osobních údajů, které zaměstnavatel vede pro účely personální a platové dokumentace (např. změnu adresy bydliště apod.).

....

Jméno a příjmení Podpis

V …….…… dne ……

Příloha 3: Souhlas se zpracováním osobních údajů – nezletilí studenti

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Tímto já .....(jméno a příjmení) jako zákonný zástupce dítěte

..... (jméno a příjmení)

d á v á m s o u h l a s se zpracováním osobních údajů

a to správci osobních údajů, kterým je Gymnázium Šternberk, sídlem Horní náměstí 5, 785 01 Šternberk, IČ 00601764, (dále jen „**Správce**“),

Osobní údaj	**Souhlas** **Nehodící škrtněte*	**Účel zpracování**
Zveřejňování fotografií ze školních akcí, výuky, soutěží apod.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zveřejňování zvukových a video záznamů.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zveřejňování výtvarných, literárních a hudebních děl vytvořených dítětem.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Informace o výsledcích soutěží a olympiád.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zpracování osobních údajů dítěte za účelem organizace školních akcí (slevy při vstupech, místní i zahraniční exkurze, apod.)	Souhlasím*/nesouhlasím*	Získání slevy na vlecích, místní i zahraniční exkurze - zajištění jízdenek k zajištění slev při vstupech.

**Nehodící škrtněte*

Osobní údaje budou zpracovány po dobu nezbytně nutnou k naplnění účelu.

**Nehodící škrtněte*

Účelem zpracování uvedených osobních údajů je informování veřejnosti o dění ve škole a propagace Správce, a to prostřednictvím internetových stránek (www.gymst.cz), oficiálních účtů Správce na sociálních sítích (facebook), tištěných materiálech, tištěných médiích a nástěnkách organizace.

S výše uvedeným zpracováním osobních údajů uděluji podpisem svobodný a výslovný souhlas. Beru na vědomí, že souhlas je dobrovolný a mohu ho vzít kdykoliv zpět, a to například datovou zprávou na schránku Správce ID webj5xm nebo dopisem na výše uvedenou adresu sídla Správce.

Prohlašuji, že jsem si vědom/a, že dle předpisů na ochranu osobních údajů mám právo:

- vzít souhlas kdykoliv zpět,
- požadovat informaci, jaké osobní údaje jsou na základě souhlasu zpracovávány,
- požadovat vysvětlení ohledně zpracování osobních údajů,
- vyžádat si přístup k těmto údajům a nechat je aktualizovat, opravit nebo doplnit,
- požadovat výmaz těchto osobních údajů,
- požadovat omezení zpracování osobních údajů,
- v případě pochybností o dodržování povinností souvisejících se zpracováním osobních údajů se obrátit na Správce nebo se stížností na Úřad pro ochranu osobních údajů (www.uoou.cz).

Podpisem zároveň stvrzuji, že další osoby oprávněné vykonávat rodičovskou odpovědnost a práva zákonného zástupce dítěte (např. druhý rodič) byly s vyjádřením takového souhlasu seznámeny a souhlasí s tím taktéž.

Více informací o tom, jak Správce zachází s osobními údaji, naleznete v dokumentu Prohlášení o ochraně osobních údajů. Dokument je dostupný v elektronické podobě na výše uvedených internetových stránkách Správce, nebo v listinné podobě v budově sídla Správce, a to v kanceláři č. 206. Funkci pověřence pro ochranu osobních údajů vykonává JUDr. Ing. et Ing. Roman Ondrýsek, Ph.D., MBA, kontakt: Schola Servis GDPR, 5b36car, Palackého 150/8, 796 01 Prostějov

.....…… ……..……

JMÉNO A PŘÍJMENÍ (TISKACÍM) PODPIS

Příloha 4: Souhlas se zpracováním osobních údajů – zletilí studenti

SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Tímto já .....(jméno a příjmení) jako **zletilý žák**

d á v á m s o u h l a s se zpracováním osobních údajů
a to správci osobních údajů, kterým je Gymnázium Šternberk, sídlem Horní náměstí 5, 785 01 Šternberk, IČ 00601764, (dále jen „**Správce**“),

Osobní údaj	**Souhlas** **Nehodící škrtněte*	**Účel zpracování**
Zveřejňování fotografií ze školních akcí, výuky, soutěží apod.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zveřejňování zvukových a video záznamů.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zveřejňování výtvarných, literárních a hudebních děl vytvořených dítětem.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Informace o výsledcích soutěží a olympiád.	Souhlasím*/nesouhlasím*	Informace veřejnosti o dění ve škole a propagace školy Správce, a to prostřednictvím oficiálních účtů Správce na sociálních sítích.
Zpracování osobních údajů dítěte za účelem organizace školních akcí (slevy při vstupech, místní i zahraniční exkurze, apod.)	Souhlasím*/nesouhlasím*	Získání slevy na vlecích, místní i zahraniční exkurze - zajištění jízdenek k zajištění slev při vstupech.

**Nehodící škrtněte*

Osobní údaje budou zpracovány po dobu nezbytně nutnou k naplnění účelu.

**Nehodící škrtněte*

Účelem zpracování uvedených osobních údajů je informování veřejnosti o dění ve škole a propagace Správce, a to prostřednictvím internetových stránek (www.gymst.cz), oficiálních účtů Správce na sociálních sítích (facebook), tištěných materiálech, tištěných médiích a nástěnkách organizace.

S výše uvedeným zpracováním osobních údajů uděluji podpisem svobodný a výslovný souhlas. Beru na vědomí, že souhlas je dobrovolný a mohu ho vzít kdykoliv zpět, a to například datovou zprávou na schránku Správce ID webj5xm nebo dopisem na výše uvedenou adresu sídla Správce.

Prohlašuji, že jsem si vědom/a, že dle předpisů na ochranu osobních údajů mám právo:

- vzít souhlas kdykoliv zpět,
- požadovat informaci, jaké osobní údaje jsou na základě souhlasu zpracovávány,
- požadovat vysvětlení ohledně zpracování osobních údajů,
- vyžádat si přístup k těmto údajům a nechat je aktualizovat, opravit nebo doplnit,
- požadovat výmaz těchto osobních údajů,
- požadovat omezení zpracování osobních údajů,
- v případě pochybností o dodržování povinností souvisejících se zpracováním osobních údajů se obrátit na Správce nebo se stížností na Úřad pro ochranu osobních údajů (www.uoou.cz).

Podpisem zároveň stvrzuji, že další osoby oprávněné vykonávat rodičovskou odpovědnost a práva zákonného zástupce dítěte (např. druhý rodič) byly s vyjádřením takového souhlasu seznámeny a souhlasí s tím taktéž.

Více informací o tom, jak Správce zachází s osobními údaji, naleznete v dokumentu Prohlášení o ochraně osobních údajů. Dokument je dostupný v elektronické podobě na výše uvedených internetových stránkách Správce, nebo v listinné podobě v budově sídla Správce, a to v kanceláři č. 206. Funkci pověřence pro ochranu osobních údajů vykonává JUDr. Ing. et Ing. Roman Ondrýsek, Ph.D., MBA, kontakt: Schola Servis GDPR, 5b36car, Palackého 150/8, 796 01 Prostějov

.....…… ……..……

JMÉNO A PŘÍJMENÍ (TISKACÍM) PODPIS

ANOTACE

Bibliografický údaj: Nováková, Vítězslava. *Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů.* Olomouc 2019. Bakalářská práce. Moravská vysoká škola Olomouc. Vedoucí práce: Ing. Lukáš Pavlík.

Název práce: Problematika GDPR a její dopady pro zaměstnavatele v oblasti ochrany osobních údajů

Autor: Vítězslava Nováková

Ústav: Ústav informatiky a aplikované matematiky

Vedoucí práce: Ing. Lukáš Pavlík

Abstrakt:

Hlavním tématem této práce je Obecné nařízení o ochraně osobních údajů známé též jako GDPR a jeho dopadem na organizace a firmy, kterých se nařízení týká. To nahradilo původní legislativu jednotlivých členských států Evropské unie zabývající se ochranou osobních dat fyzických osob. GDPR je v současné době platnou legislativou na celém území EU. Nová legislativa vyžaduje od všech organizací dokumentaci způsobu, jakým způsobem a z jakého důvodu jsou osobní údaje zpracovávány a posiluje práva subjektů. Cílem této práce je implementace Obecného nařízení o ochraně osobních údajů ve vybrané společnosti – Gymnáziu Šternberk.

Školy obecně zpracovávají velké množství osobních údajů. Mezi ty patří údaje o studentech, jako jsou známky, údaje o zdravotním stavu, fotografie a další. Školy také uchovávají údaje o svých zaměstnancích a uchazečích o zaměstnání a také o třetích osobách jako jsou dodavatelé. Školy dále zpracovávají tzv. citlivé osobní údaje, které jsou důsledněji regulovány. Může se jednat o údaje o rase, etnickém původu, biometrické údaje či zdravotní dokumentaci. Aby bylo vyhověno požadavkům GDPR, je třeba, aby každá škola sbírala a uchovávala data pouze ze zákonných důvodů.

K dosažení souladu s Nařízením je nutno zavést v organizacích nové systémy ke zpracovávání osobních údajů, proškolit zaměstnance a přijmout různá další opatření. Ta všechna je však stojí čas i peníze. Tato práce se zabývá opatřeními přijatými Gymnáziem Šternberk a dále doporučuje další vylepšení ke zlepšení ochrany osobních údajů.

Klíčová slova: osobní údaje, Obecné nařízení o ochraně osobních údajů, GDPR, ochrana osobních dat, subjekt osobních údajů, správce osobních údajů, zaměstnavatel, zaměstnanci, žáci

---

Title: The Issue of GDPR and its Impact on Employers in the Field of Personal Data Protection

Author: Vítězslava Nováková

Department: Department of Computer Science and Applied Mathematics

Supervisor: Ing. Lukáš Pavlík

Abstract:

The main topic of this thesis is the General Data Protection Regulation also known as GDPR and its impact on the organizations and companies to which the regulation is concerned. The Regulation has replaced the original legislation of the individual member states of the European Union dealing with the protection of personal data. The GDPR is now recognised as law across the EU. The new legislation requires all organisations to document how and why they process all personal data, and gives enhanced rights to the individual. The main objective of this thesis is the implementation of the General Data Protection Regulation in the selected organisation – Šternberk Highschool.

Schools in general handle a large amount of personal data. This includes information on students, such as grades, medical information, images and much more. Schools will also hold data on staff and job applicants and also external third parties such as contractors. Schools will also handle what the GDPR refers to as special category data, which is subject to tighter controls. This could be details on race, ethnic origin, biometric data or medical records. To meet the GDPR, every school must have a lawful basis for collecting and holding personal data.

Achieving compliance with the GDPR requires documenting every system used to process personal data, introducing new systems, staff training and other measures. All of these take time and money. This thesis documents measures adopted by Šternberk Highschool and suggests further improvements of personal data protection.

Keywords: Personal Data, General Data Protection Regulation, GDPR, Privacy Policy, Personal Data Subject, Data protection Officer, Employer, Employees, Students