Univerzita Karlova
Pedagogická fakulta

Katedra andragogiky a managementu vzdělávání

BAKALÁŘSKÁ PRÁCE

Ochrana osobních údajů ve škole

Personal data protection at school

Jakub Varga

Vedoucí práce: RNDr. Ing. Eva Urbanová, Ph.D., MBA

Studijní program: Školský management

Studijní obor: Školský management

2023

Odevzdáním této bakalářské práce na téma Ochrana osobních údajů ve škole potvrzuji, že jsem ji vypracoval pod vedením vedoucí práce samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 9. 7. 2023

Děkuji vedoucí práce paní RNDr. Ing. Evě Urbanové, Ph. D., MBA za cennou pomoc při psaní této bakalářské práce. Za její postřehy a zkušenosti. Dále děkuji všem, kteří se podíleli na praktické části zejména pak respondentům kvantitativního výzkumu.

ABSTRAKT

Bakalářská práce se zaměřuje na ochranu osobních údajů ve školách a analyzuje způsoby, jak zajišťovat jejich bezpečnost. Teoretická část práce se zabývá základními pojmy z oblasti osobních údajů a jejich ochranou, včetně souvisejících aspektů GDPR (Obecné nařízení o ochraně osobních údajů) a role pověřence pro ochranu osobních údajů.

Práce se dále věnuje popisu možností úniku osobních údajů a nabízí řešení pro jejich prevenci. Zkoumá také výhody a nevýhody využití pověřence pro ochranu osobních údajů v rámci školního prostředí.

V praktické části práce je proveden kvantitativní výzkum prostřednictvím dotazníkového šetření, které zkoumá, jak jsou osobní údaje chráněny ve vedení škol. Cílem tohoto šetření je získat informace o stávajících postupech, používaných opatřeních a povědomí vedení škol o problematice ochrany osobních údajů.

Na základě výsledků získaných v průběhu výzkumu bude vypracován návrh řešení pro ochranu osobních údajů ve školách. Tento návrh bude zvláštní pozornost věnovat možným rizikům úniku osobních údajů a navrhne opatření, která by měla být přijata k jejich minimalizaci.

Výsledkem bakalářské práce bude ucelený přehled o problematice ochrany osobních údajů ve školách a konkrétní návrh řešení, který může být využit v praxi. Tato práce přispěje k lepšímu porozumění ochrany osobních údajů ve školství a může sloužit jako podklad pro další výzkum nebo implementaci opatření v oblasti ochrany osobních údajů ve školách.

KLÍČOVÁ SLOVA

GDPR, škola, ochrana osobních údajů, pověřenec

ABSTRACT

The bachelor's thesis focuses on the protection of personal data in schools and examines ways to ensure their security. The theoretical part of the thesis deals with fundamental concepts related to personal data and their protection, including key aspects of the General Data Protection Regulation (GDPR) and the role of the Data Protection Officer.

The thesis further describes the possibilities of personal data breaches and offers solutions for their prevention. It also explores the advantages and disadvantages of employing a Data Protection Officer within the school environment.

In the practical part of the thesis, a quantitative research using a questionnaire survey is conducted to investigate how personal data protection is ensured in school management. The aim of this survey is to gather information about current practices, implemented measures, and the awareness of school management regarding the issues of personal data protection.

Based on the results obtained during the research, a proposal for personal data protection in schools will be developed. This proposal will pay special attention to potential risks of data breaches and suggest measures that should be taken to minimize them.

The outcome of the bachelor's thesis will be a comprehensive overview of the issues related to the protection of personal data in schools, along with a concrete proposal for a solution that can be implemented in practice. This work will contribute to a better understanding of personal data protection in the field of education and can serve as a basis for further research or the implementation of measures in the area of personal data protection in schools.

KEYWORDS

GDPR, school, personal data protection, officer

Obsah

Úvod

Každý občan České republiky je nucen a povinen poskytovat své osobní údaje jiným stranám během svého života, a to při uzavírání smluv, pojištění, vyřizování dokumentů a při různých administrativních úkonech. Tyto údaje jsou zneužitelné a lidé si často neuvědomují nebo nechtějí připustit potenciální riziko jejich zneužití.

Zneužití citlivých dat může nastat snadno, a to jak v reálném světě, tak v kyberprostoru prostřednictvím hackerských útoků. Proto Evropská unie, do které Česká republika patří od roku 2004, podnikla kroky k ochraně osobních údajů. V první polovině roku 2018 vstoupilo v platnost Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Revoluční a nová legislativa Evropské unie měla jako cíl významně posílit ochranu osobních údajů svých občan. Součástí tohoto nařízení se stalo i přijetí Obecného nařízení o ochraně osobních údajů (dále jen Nařízení GDPR z anglického General Data Protection Regulation). „*GDPR představuje nový právní rámec ochrany osobních údajů v evropském prostoru s cílem hájit co nejvíce práva občanů EU proti neoprávněnému zacházení s jejich daty včetně osobních údajů. GDPR se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data uživatelů*.“ (Nařízení Evropského parlamentu a Rady (EU) 2016/679, online).

Mimo ochranná opatření, implementovalo Nařízení GDPR do legislativ všech členských zemí Evropské unie i velmi vysoké finanční pokuty pro ty subjekty, které budou porušovat daná pravidla a nařízení. Mimo jiné nařizuje některým správcům nebo zpracovatelům osobních údajů, aby zřídili nezávislou kontrolní funkci, která je známa pod zkratkou DPO (Data Protection Officer, tj. pověřenec pro ochranu osobních údajů).

Vzdělávací instituce, jako jsou školy, zpracovávají velké množství osobních údajů velkého počtu lidí, kteří je navštěvují, pracují nebo se do nich hlásí. Tyto instituce jsou tedy povinny řídit se Nařízením GDPR, jehož cílem je v případě vzdělávacích institucí chránit práva žáků a jejich zákonných zástupců, zaměstnanců i uchazečů před neoprávněným zacházením s jejich údaji a dát jim větší kontrolu nad tím, co se s nimi děje.

Další povinností vzdělávacích institucí jako orgánů veřejné moci, které se zabývají právy a povinnostmi dětí, žáků nebo studentů, je jmenovat pověřence pro ochranu osobních údajů nebo třetí nezávislou stranu, která se bude věnovat zpracování a ochraně a ukládání osobních údajů. Tuto osobu jmenuje ředitel dané školy.

Cílem bakalářské práce s názvem Ochrana osobních údajů ve škole je navrhnout řešení pro ochranu osobních údajů ve školách s důrazem na možný únik těchto údajů.

Bakalářská práce se skládá z teoretické a praktické části. Teoretická část zahrnuje vysvětlení základních pojmů týkajících se GDPR, které objevují v celé práci. Také je podrobněji popsán legislativní rámec Nařízení GDPR a role pověřence GDPR, který hraje důležitou roli v ochraně osobních údajů ve školách. Druhá kapitola se zaměřuje na implementaci Nařízení GDPR do vzdělávacích institucí, popsání povinnosti, které jsou na školy kladené a roli pověřence GDPR v ochraně osobních údajů žáků a studentů.

V rámci výzkumné části bakalářské práce je proveden kvantitativní výzkum formou dotazníkového šetření. Dotazníkové šetření zjišťuje, jakým způsobem vedení současných českých škol zajišťuje ochranu osobních údajů svých studentů. Informace získané z dotazníku jsou analyzovány pomocí předem stanovených výzkumných otázek. Ty konkrétně zní následovně:

1. Jakým způsobem vedení školy chrání osobní údaje ve škole?
2. Proč je vhodný k delegování ochrany osobních údajů pověřenec GDPR?
3. V jakých nejčastějších případech dochází k únikům osobních údajů ze škol?

1 Ochrana osobních údajů v souladu s Nařízením GDPR

Předtím, než se bakalářská práce zaměří na problematiku ochrany osobních údajů a Nařízení GDPR v rámci vzdělávacích institucí, budou definovány základní pojmy, které s touto problematikou bezprostředně souvisejí. Konkrétně bude charakterizováno, co jsou osobní údaje, co je ochrana osobních údajů, co je Nařízení GDPR, potažmo, co znamená, když jsou osobní údaje zneužity.

1.1 Základní pojmy

Osobní údaje

Osobními údaji v současné době disponuje každý člověk na této planetě. Pro každého člověka jsou osobní údaje specifické a individuální. Snaha lidi na této planetě nějakým způsobem oficiálně identifikovat je lidstvu vlastní již po mnohá staletí, avšak právě v posledních několika desetiletích význam osobních údajů velice narostl, stejně jako snaha tyto osobní údaje ochraňovat před zneužitím nebo krádeží (Matoušová a Hejlík, 2008, s. 53).

Jakým způsobem lze odborně definovat osobní údaje? Je důležité si uvědomit, že existuje mnoho různých definic osobních údajů v literatuře i právních předpisech. Tato bakalářská práce se však bude opírat především o definice, které lze nalézt v mezinárodních nebo státních nařízeních anebo v legislativě.

Pod pojmem osobní údaje lze chápat jako veškeré informace, které existují o identifikované nebo identifikovatelné fyzické osobě, která je z legislativního hlediska označována za subjekt údajů (Článek 4 odst. 1 Obecného nařízení, online).

Konkrétně za osobní údaje se považuje „*každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.* (MVČR, online, 2000).

Za zcela zcestné je možné považovat, pokud se někdo domnívá, že osobními údaji představují pouze jméno, příjmení, datum narození, adresu trvalého bydliště, číslo občanského průkazu, popřípadě rodné číslo konkrétního jedince. Je nutné chápat, že osobních údajů existuje velké množství, a každý člověk bez rozdílu těmito zcela individuálními údaji disponuje (Matoušová a Hejlík, 2008).

Citlivý údaj

Citlivý údaj je specifický druh osobního údaje, který zahrnuje nejen běžné informace o fyzické osobě, ale také údaje, které mají zvláštní vlastnosti. Tyto informace poskytují hloubkový pohled do soukromí jednotlivce a jsou intenzivnějšího charakteru. Proto se také kladou vyšší požadavky na ochranu těchto údajů a existují přísnější podmínky pro jejich zpracování.

Za citlivý údaj nebo citlivý osobní údaj lze konkrétně považovat „…*údaj, který vypovídá o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filosofickém přesvědčení nebo členství v odborové organizaci, genetický údaj, biometrický údaj zpracovávaný za účelem jedinečné identifikace fyzické osoby, údaj o zdravotním stavu, o sexuálním chování, o sexuální orientaci a údaj týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření.*“ (§ 66 zákona č. 111/2019 Sb.).

Zpracování osobních údajů

Každý subjekt údajů je jedinečným vlastníkem svých osobních údajů. Nicméně, lidé dennodenně poskytují své osobní údaje třetím stranám, jako jsou státní nebo soukromé instituce, prodejci nebo jiné subjekty. Tyto subjekty pak sbírají shromážděné informace o jednotlivcích.

Legislativní pojetí pojmu zpracování osobních údajů se nevztahuje na jakékoli manipulaci s cizími osobními údaji. Za zpracování osobních údajů lze chápat sofistikovanou činnost, které není v žádném případě nahodilá, ale která je správci osobních údajů prováděna s konkrétním účelem, a je činěna současně systematicky (Úřad pro ochranu osobních údajů, online, 2017).

Zákon o zpracování osobních údajů rozděluje povinnosti při zpracování těchto také na 2 účely.

- „*za účelem vědeckého nebo historického výzkumu nebo pro statistické účely*“ a
- „*pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu*“ (Zákona č. 110/2019 Sb.).

Ochrana osobních údajů

V současné době má v rámci vyspělých civilizací každá osoba právo na ochranu svých osobních údajů, a především disponuje právem na ochranu těchto údajů při tom, když jsou zpracovávány jiným subjektem. Právo na ochranu osobních údajů se vyvíjí spolu s lidskou civilizací, avšak je zapotřebí si uvědomit, že s tímto konceptem začalo být pracováno až v rámci 19. století (Mates a kolektiv, 2012, s. 29).

Nepřeberné a neustále narůstající množství informací, které je každodenně na celém světě v současné době zpracováváno a obsahuje osobní údaje, je typické až pro dnešní moderní a současně i technologicky vyspělou dobu, kde se značná část činností odehrává v rámci kybernetického prostoru. Nutnost chránit osobní údaje tak úměrně narůstá s rozmachem informačních technologií, a se vzrůstajícím ekonomickým významem osobních údajů v rámci kybernetického světa. Na internetu je v současné době realizován značný podíl peněžních transakcí a prodejů, při kterých jsou spotřebiteli odesílány osobní údaje, které mohou být potencionálně zneužity (Mates a kolektiv, 2012, s. 31).

V případě, že nejsou osobní údaje dostatečným způsobem chráněny, vzniká značné riziko jejich potencionálního a neoprávněného využití, popřípadě i zneužití pro páchání trestné činnosti (Navrátil a kolektiv, 2018, s. 102).

Prvním základním mezinárodním dokumentem, v rámci, kterého byla ochrana osobních údajů řešena, byla Úmluva Rady Evropy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat, k jejímuž přijetí došlo roku 1981. Tento dokument jako vůbec první jasně charakterizoval základní termíny, které s ochranou osobních dat souvisejí (tzn. osobní údaj, automatizované zpracovávání dat), a mimo to v tomto dokumentu došlo i ke stanovení základních pravidel a nařízení pro zpracování osobních údajů, stejně jako úmluva vyzdvihovala potřebu pevného zabezpečení těchto

zpracovávaných dat. Nutné je podotknout, že mnoho v tomto dokumentu stanovených pravidel a nařízení je platných i v současné době, 4 let po jeho přijetí (Žůrek, 2017, s. 13-18).

Dlouhou dobu byla výše uvedená směrnice jediným platným právním předpisem na území Evropy. Nicméně, s rozvojem informačních technologií, rostoucím počtem přenášených a zpracovávaných dat a údajů, se ukázala jako nedostatečná. Navíc, stále intenzivnější volný pohyb osob v rámci Evropské unie se stával nekontrolovatelným. Nesourodost právních předpisů jednotlivých členských zemí EU na toto téma, donutilo Evropskou unii přijmout roku 1995 Směrnici Evropského parlamentu a Rady (EU) 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Přijetím této směrnice došlo ve všech členských státech EU ke sjednocení legislativy týkající se ochrany osobních údajů (Žůrek, 2017, s. 13-18).

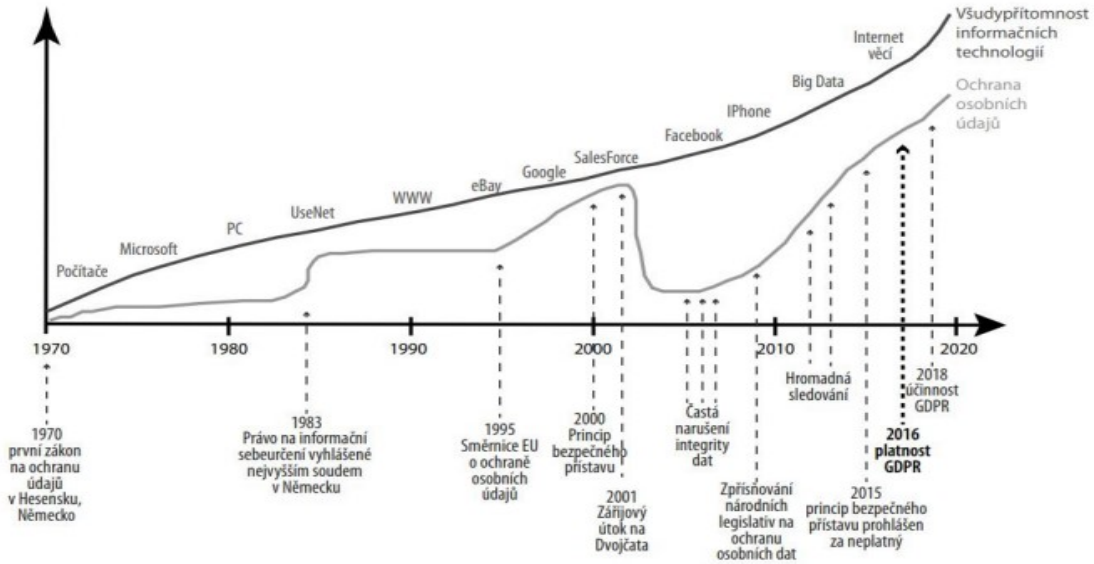
Nutno dodat, že i Česká republika, ačkoliv nebyla ještě plnohodnotným členem EU, přijala již roku 2000 zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, ve kterém došlo k vymezení základních pojmů týkajících se této problematiky, stejně jako k sepsání práv a povinností při zpracovávání osobních údajů cizí stranou nebo pravidla pro předávání údajů do zahraničí. Prostřednictvím přijetí tohoto zákona také došlo k ustanovení státní instituce, která se bude touto problematikou a jejím dozorováním zabývat. Touto institucí se stal Úřad pro ochranu osobních údajů.

Protože nastával další významný rozvoj internetu, internetových transakcí a obchodů, musela na to reagovat i Evropská unie, která byla nucena změnit stávající směrnice a nařízení. Z toho důvodu vešlo od roku 2018 v platnost Obecné nařízení o ochraně osobních údajů, které rušilo všechny stávající směrnice, a které byly všechny členské státy povinné implementovat do svých legislativ. Spolu se zmíněným Obecním nařízením alias GDPR, vešly v platnost další dvě dodatkové směrnice. Konkrétně se jednalo o přijetí:

- Směrnice Evropského parlamentu a Rady s označením 2016/680, trestněprávní směrnice, pro oblast ochrany fyzických osob v souvislosti se zpracováním osobních údajů za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů.

- Směrnice Evropského parlamentu a Rady s označením 2016/681, směrnice PNR (Passenger Name Record) pro oblast používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnost.

Obrázek 1: Vztah rozvoje internetu a nutnosti chránit osobní údaje.



Zdroj: Nezmar 2017.

Grafické znázornění v Obrázku 1 ukazuje, že nutnost ochrany osobních údajů roste s rozvojem internetových aktivit. Informační technologie se však vždy vyvíjejí rychleji než legislativní opatření k jejich ochraně. Ty vždy přicházejí až reakcí na danou technologii nebo na nebezpečnou událost, kdy bylo například ohroženo odcizení osobních údajů. (Nezmar 2017, s. 15)

GDPR

Důležitým dotazem před implementací evropského GDPR v roce 2018 bylo proč Evropa potřebuje vylepšenou ochranu osobních dat a proč předchozí směrnice nebyla dostatečná. Toto již bylo zodpovězeno v předchozích kapitolách. Nová legislativa reaguje na trend v masivním růstu informačních technologií a jejich zintenzivněný význam.

V dřívějším rozhodnutí nebyly brány v úvahu proměnné, které se objevily až později, jako např. cloudová úložiště a nevyřešené sociální sítě. Odborníci se shodují, že nové směrnice zaostávají za technologickým vývojem asi o 5 let.

„*Obecné nařízení na ochranu osobních údajů neboli GDPR (General Data Protection Regulation) je dosud nejvíce uceleným souborem pravidel na ochranu dat na světě. GDPR se dotýká každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu*“ (Škorničková, 2018).

GDPR je tedy možné chápat jako všeobecně platným nařízením, který se týká jednotlivců, firem a institucí, zapojených do zpracování osobních údajů. To mohou být zaměstnavatelé, dodavatelé, prodejci, klienti i spotřebitelé. GDPR se vztahuje na všechny sektory a odvětví. Také se týká těch, kteří analyzují chování lidí na internetu prostřednictvím technologií. Hlavním cílem GDPR je ochránit digitální práva občanů celé Evropské unie (Škorničková 2018).

Správce osobních údajů

Ve 4 článku Nařízení GDPR je stanoveno, že správce představuje osobu, která je „*fyzickou nebo právnickou osobou, orgánem veřejné moci, agenturou nebo jiným subjektem, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení*“.

Správce tedy může zajistit zpracování, sběr a ochranu osobních údajů pomocí zpracovatele.

Zpracovatel osobních údajů

Ve 4 článku Nařízení GDPR je stanoveno, že zpracovatel je „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce*“.

1.2 Legislativa

V této kapitole se zaměříme na Obecné nařízení o ochraně osobních údajů (2016/679/EU), též známého jako GDPR (General Data Protection Regulation). Nařízení bude podrobně

rozebráno a představí se novinky, které přináší ve srovnání s dřívější směrnicí, implementovanou českým zákonem o ochraně dat z roku 2000, zákonem č. 101/2000 Sb., a později jejich zpracováváním z roku 2019, zákonem č. 110/2019 Sb.

Obecné nařízení o ochraně osobních údajů (2016/679/EU), známé jako GDPR, ovlivňuje mnoho oblastí života, ekonomiky a práva v Evropské unii. Tyto oblasti jsou povinny dodržovat unijní právní předpisy. Výjimkou jsou policejní aktivity a orgány zabývající se trestním řízením (MPO ČR 2018).

Až do roku 2019 byla ochrana soukromých informací na území Česka regulována zákonem č. 101/2000 Sb., implementujícím evropskou směrnici z roku 1995. GDPR vychází z této směrnice a stává se pro něj klíčovým zdrojem. Struktura obou norem a klíčové body zůstávají v obou dokumentech podobné (MPO ČR 2018).

Po úvodních definicích klíčových pojmů, se Obecné nařízení o ochraně osobních údajů (2016/679/EU), často známé jako GDPR, zaměřuje na specifické principy, pravidla a předpisy týkající se ochrany osobních údajů. Tento právní akt následně vymezuje specifická práva subjektu údajů a povinnosti správců, zpracovatelů a dalších stran, které se zabývají zpracováním osobních údajů. Tyto povinnosti se týkají jak technických, tak i právních aspektů zpracování osobních údajů, aby byla zajištěna maximální možná ochrana těchto dat. Kromě toho se GDPR také zabývá otázkou mezinárodního převodu osobních údajů, rolí dozorových úřadů a soudní ochrany práv subjektů údajů. Dále je pozornost zaměřována i na mezinárodní převody osobních údajů, na aktivitu dozorových úřadů či soudní a správní ochranu viz Obecné nařízení o ochraně osobních údajů (2016/679/EU)).

I když jsou obě směrnice podobné, v novém předpisu došlo k výrazným změnám. Ty se týkají i zavedení nových povinností pro zpracovatele a správce osobních dat, jako je například povinnost vytvořit záznamy o zpracování jednotlivých údajů, nebo možnost jmenovat tzv. pověřence pro ochranu osobních údajů v určitých případech (Obecné nařízení o ochraně osobních údajů (2016/679/EU)).

V rámci této bakalářské práce nebude pozornost věnována nařízením nebo povinnostem, které byly novým nařízením přejaty z původní směrnice, ale budou vyjmenovány nové oblasti a povinnosti, kterým se zaobírá GDPR, a kterým se nevěnovala směrnice z roku 1995.

V této bakalářské práci budou detailně zkoumány nové aspekty a povinnosti, na které se zaměřuje Nařízení GDPR, ale nebyly součástí starší směrnice z roku 1995:

- Tzv. právo být zapomenut (v rámci článku 17).
- Tzv. právo na přenositelnost osobních údajů (v rámci článku 20).
- Podrobnější definice vztahu správce a zpracovatele k subjektům údajů.
- Zvýšená kontrola správců osobních údajů mimo půdu Evropské unie.
- Stanovení dalších povinností správcům a zpracovatelům osobních dat (např. hodnocení dopadů manipulace s osobními daty na soukromí subjektů těchto údajů či povinné konzultace s dozorovým orgánem).
- Zrušení nutnosti notifikovat všechna nová zpracování osobních údajů u dozorového orgánu.
- Zesílení intenzity zabezpečování dat, co se především technického hlediska týče.
- Povinnost nahlašovat narušení bezpečnosti osobních dat.
- Nutnost jmenovat pověřence pro ochranu osobních údajů pro veřejnou správu a pro část společností.
- Podrobnější úprava nástrojů soft law (tzn. kodexy, certifikace)
- Sjednocení pravomocí úřadů pro ochranu osobních údajů ve všech zemích EU.
- Detailnější definice spolupráce jednotlivých dozorových úřadů v EU.
- Zavedení vzájemného rozhodování dozorových úřadů v případě přeshraničních případů.
- Zavedení rozhodovací pravomoci Evropského sboru dozorových úřadů v záležitostech, ve kterých nedojde ke stanovení společného rozhodnutí dozorových úřadů.
- Navýšení a současné sjednocení sankcí při porušení pravidel ochrany osobních údajů (konkrétně v hodnotě 2 % nebo dokonce 4 % podílu z ročního globálního obratu konkrétního podniku, popřípadě až v hodnotě 20 mil. eur).
- Úpravy, které mají za cíl vytvořit fungující vztah mezi právem občanů na ochranu jejich osobních údajů a jejich právem na svobodu projevu.

Český zákon o ochraně dat z roku 2000, zákon č. 101/2000 Sb. byl roku 2019 zrušen a následně nahrazen zákonem č. 110/2019 Sb. „*Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů*“ (Zákon 110/2019 Sb.).

Nejvíce zásadním rozdílem mezi zákonem č. 101/2000 Sb., a v současné době aktuálním zákonem č. 110/2019 Sb., je, že blíže specifikuje některá ustanovení 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 (dále jen „GDPR“).

Všeobecně však lze říct, že přijaté novinky v právní úpravě ochrany osobních údajů nebyly nijak zásadního rázu a měly převážně povahu zpřesnění stávající úpravy v tematicky ohraničených oblastech. Z pohledu veřejných subjektů a orgánů veřejné moci však zákon č. 101/2000 Sb. přináší významné úlevy, zejména z hlediska omezení možností správního trestání. Lze tak říct, že všechny prvky zmíněné v zákoně č. 101/2000 Sb. v zákoně z roku 2019 zůstaly, avšak byly více upřesněny a ohraničeny v jednotlivé oblasti.

Hlavními změnami, ke kterým v novém zákoně č. 110/2019 Sb. oproti původnímu zákonu č. 101/2000 Sb., došlo, jsou:

- Upřesnění pojmu „veřejný subjekt“
- Stanovení věkové hranice
- Upřesnění výjimek
- Zpracování údajů pro novinářské a umělecké účely
- Upřesnění přestupků a sankcí

1.3 Pověřenec GDPR

V rámci nového nařízení GDPR je zavedena role pověřence pro ochranu osobních údajů, který se také nazývá Data Protection Officer (DPO). Hlavním důvodem, proč byl pověřenec pro ochranu osobních dat zaveden je, že se jedná o osobu, tzv. třetí neutrální a nezávislou stranu, která bude stát mezi konkrétními subjekty, s jejichž osobními údaji je operováno, a podnikem/ veřejnou institucí, která by data za normálních okolností zpracovávala a uchovávala (Škorničková, 2018).

Tento pověřenec má jako svůj hlavní úkol monitorovat dodržování povinností týkajících se zpracování osobních údajů stanovených v GDPR, a zajistit jejich harmonii (Škorničková, 2018).

Neutrální a nestranná osoba v podobě pověřence pro ochranu osobních údajů však nemusí být jmenována všemi institucemi nebo všemi podniky. K jejich jmenování dochází ve třech konkrétních situacích, a to, pokud (Obecné nařízení o ochraně osobních údajů (2016/679/EU)):

- Má zpracování osobních údajů za povinnost provést některý z orgánů veřejné moci, popřípadě či veřejný subjekt (s výjimkou soudů),
- By musel správce nebo zpracovatel osobních údajů za úkol zpracovat velké množství dat, a to v pravidelném intervalu, nebo pokud se jedná o plošné monitorování občanů.
- By správce nebo zpracovatel osobních údajů musel zpracovávat rozsáhlé množství zvláštních údajů, popřípadě osobních údajů, které se týkají trestné činnosti, popřípadě rozsudků v trestních záležitostech.

U všech třech bodů se jedná o situace, kdy by měl být běžný správce nebo zpracovatel osobních údajů veden osobou, která disponuje odbornými znalostmi týkající se legislativních předpisů a postupů, které mají, co dočinění s ochranou osobních dat. Pověřenci pro ochranu osobních údajů mohou být externími pracovníky, kteří zpracovávají data pro společnost nebo instituci, avšak může se jednat i o vyškoleného zaměstnance této společnosti/ organizace. Ať již se jedná o první nebo druhou možnost, vždy by měl být pověřenec nestranný, nezávislý a profesionální (Nulíček a kolektiv, 2018, s. 359-365).

Pověřenec pro ochranu osobních údajů ve veřejném sektoru může být jak fyzická, tak právnická osoba, která byla pověřena prováděním tohoto úkolu podle předpisů GDPR. Tento pověřenec může vystupovat jako ochránce osobních údajů pro více státních institucí nebo firem, pokud jsou tyto subjekty podobně strukturovány. Avšak každý z těchto subjektů, kterému pověřenec vystupuje, musí mít určité společné prvky (Nulíček a kolektiv, 2018, s. 365-367).

Pověřenec pro ochranu osobních údajů je v rámci Nařízení GDPR spravován v rámci článku 37, ve kterém jsou vyjmenovány konkrétní požadavky, které jsou z odborného hlediska na pověřence kladeny. Není zde jasně definováno, jakého vzdělání nebo odbornosti je povinen pověřenec docílit, aby mohl povolání vykonávat, nicméně je zde jasně stanoveno, že by měl disponovat odpovídajícími znalostmi z právního hlediska, i z hlediska ochrany osobních údajů (znalost evropského práva, znalost českého práva, znalost informačních systémů a

technologií). Správcům a zpracovatelům osobních údajů je dokumentem nařizováno, aby zveřejňovali kontaktní údaje svého pověřence. Ty musí být předány i Úřadu pro ochranu osobních dat (Obecné nařízení o ochraně osobních údajů (2016/679/EU)).

Následně článek 39 Obecného nařízení o ochraně osobních údajů (2016/679/EU) dále vyjmenovává základní úkoly, které musí pověřenec uskutečnit. Mezi tyto konkrétně patří:

- „*Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle Nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů*“ (Článek 39 odst. 1 písm. a).

- „*Monitorování souladu s Nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany osobních údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů*“ (Článek 39 odst. 1 písm. b).

- „*Poskytování poradenství na žádost, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35*“ (Článek 39 odst. 1 písm. c).

- Spolupráce s dozorovým úřadem (Článek 39 odst. 1 písm. d).

- „*Působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoliv jiné věci*“ (Článek 39 odst. 1 písm. d).

Obrázek 2: Pozice pověřence pro ochranu osobních údajů je podle GDPR silná, a jsou na něj kladeny současně i vysoké nároky.

Zdroj: https://privacydesk.in/

2 Implementace Nařízení GDPR do škol

Vzdělávací instituce jsou zákonem povinny dodržovat nařízení Evropské unie zvané GDPR. Toto nařízení má za cíl chránit práva žáků a jejich zákonných zástupců před možným neoprávněným zacházením s jejich osobními údaji, a poskytnout jim větší kontrolu nad tím, jak jsou jejich údaje využívány. Vzdělávací instituce, jako instituce veřejné moci, také rozhodují o právech a povinnostech širokého spektra dětí, žáků a studentů, a z tohoto důvodu jsou povinny jmenovat pověřence pro ochranu osobních údajů, který bude odpovědný za řízení a správu těchto údajů. Pověřenec pro ochranu osobních údajů je jmenován ředitelem dané instituce.

Ve druhé kapitole bakalářské práce se bude zaměřovat na základní povinnosti školy v oblasti ochrany osobních údajů svých studentů podle nařízení GDPR, stejně jako na specifickou roli pověřenců pro ochranu osobních údajů v institucích škol.

2.1 Základní povinnost škol v ochraně osobních údajů

V každém stupni vzdělávacích institucí dochází k systematickému zpracování velkého množství osobních dat, jako jsou osobní údaje samotných žáků, studentů, jejich právních zástupců, potenciálních uchazečů, a dokonce i zaměstnanců. Tyto instituce se musí držet aktuálních zákonů a v roce 2018 byly povinny přijmout a implementovat Nařízení GDPR, které jim ukládá nové povinnosti týkající se ochrany osobních údajů všech dotčených osob, jejichž data jsou shromažďována a zpracovávána.

V oblasti vzdělávání, jako i v jiných veřejných institucích či soukromých podnicích, je nutné dodržovat základní zásady a povinnosti stanovené v článku 5. Tyto zásady a povinnosti se stávají východiskem pro všechny další úkony spojené se zpracováváním a manipulací s osobními údaji. Jedná se konkrétně o tyto principy (Článek 5):

- Princip zákonnosti, korektnosti a transparentnosti,
- Princip účelového omezení,
- Princip minimalizace údajů,
- Princip přesnosti,
- Princip omezení uložení,

- Princip integrity a důvěrnosti,
- Princip odpovědnosti.

Princip zákonnosti, korektnosti a transparentnosti

První zásada ochrany osobních údajů je podle mnoha odborníků současně tou nejvíce zásadní (Nulíček a kolektiv, 2018, s. 105-106). V pátém článku GDPR je uvedeno, že osobní údaje musí být „*ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem*“.

V článku 6 Obecného nařízení o ochraně osobních údajů (2016/679/EU) jsou sepsána základní pravidla, která musí být dodržována:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

Princip účelového omezení

Dle tohoto principu je stanoven způsob, jakým má správce osobních dat zpracovávat a nakládat s těmito informacemi. Tento bod je důležitý, jelikož vytváří základ pro další povinnosti týkající se ochrany osobních dat. Stanovení účelu pro zpracovávání osobních dat je klíčové a mělo by být provedeno s pečlivostí.

V článku 5 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že osobní údaje musí být „*shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely.“*

Především je nutné určit specifický, jasný a oprávněný účel zpracování osobních údajů. Při stanovení právního základu pro zpracování konkrétních osobních dat je třeba zajistit, aby z toho bylo jasně zřejmé, pro jaké účely se data zpracovávají. Je nutné zjistit, z jakého důvodu se data shromažďují, na co se použijí a jakým způsobem budou sloužit (Nulíček a kolektiv, 2018, s. 118-120).

Stanovení důvodu shromažďování osobních údajů musí být provedeno před zahájením samotného shromažďování. Je neodpustitelné shromažďovat osobní data bez vědomí jednotlivců, od kterých jsou shromažďována, a bez informování jich o účelu této činnosti. Není povoleno stanovit účel dodatečně. Tento účel musí být výslovně oznámen všem subjektům, od kterých jsou data shromažďována. Správce a zpracovatel dat nesmí využívat osobní údaje ke jiným účelům, než k jakým byly legálně shromažďovány a sbírány (Nulíček a kolektiv, 2018, s. 120-122).

Princip minimalizace údajů

V článku 5 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že osobní údaje musí být „*přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány*.“

Po stanovení jasného účelu shromažďování a sbírání osobních údajů správcem nebo zpracovatelem, je nutné při každé příležitosti ověřovat, zda je nutné realizovat všechny plánované akce k dosažení tohoto účelu a zda není získáváno více informací, než je nezbytně nutné (Nulíček a kolektiv, 2018, s 134-135).

Významem předchozího je, že správce a zpracovatel osobních údajů by měl shromáždit jen nezbytné informace k vyhodnocení nebo analýze. Pokud bude vzdělávací instituce shromažďovat osobní údaje k získání kontaktů na zákonné zástupce studentů, nebude se na ně dotazovat na jejich rodné číslo, jelikož tento údaj není důležitý pro primární účel shromažďování dat. Cílem bylo získat kontaktní informace na studenty, a z tohoto důvodu se budou dotazovat na telefonní číslo nebo e-mailovou adresu jejich rodičů (Nulíček a kolektiv, 2018, s. 137).

Princip přesnosti

V článku 5 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že osobní údaje musí být „*přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny*."

Co je konkrétně nařízením chápáno jako přesné, zde není definováno. Odborníci však dodávají, že za nepřesné údaje lze považovat takové údaje, které jsou nejasné, matoucí, nepravdivé, přímo lživé nebo zavádějící (Nezmar, 2017, s. 63, Nulíček a kolektiv 2017). Správce nebo zpracovatel osobních údajů má ze zákona povinnost kontrolovat získané údaje, a v případě, že přijde na to, že se jedná o nepřesné údaje, má za povinnost tyto údaje vymazat nebo náležitě opravit (Nulíček a kolektiv, 2018, s. 148-150).

Princip omezení uložení

V článku 5 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že osobní údaje musí být „*uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za*

předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.“

Výstižně řečeno, správci a zpracovatelé osobních údajů by měli zajistit, aby bylo udržováno osobní údaje jen po takovou dobu, která je nutná k dosáhnutí hlavního cíle jejich shromažďování. Chcete-li dodržet první pravidlo, by měl být původce dat informován o tom, jak dlouho bude s jeho osobními údaji nakládáno a jak dlouho budou uchovávány. Pokud nelze určit přesné datum, je možné subjekt také informovat o potenciálním datu, např. u vzdělávacích institucí se obvykle jedná o dobu do konce studia. Však nelze stanovit dobu jako neurčitou, vždy musí být stanoven minimálně relativní časový úsek. Tyto doby, jak konkrétní, tak relativní, musí být kontrolovány a zabráněno překročení termínů (Nulíček a kolektiv, 2018, s. 157-160).

Princip integrity a důvěrnosti

V článku 5 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že osobní údaje musí být „*zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením*.“.

Organizace, instituce nebo firma, která si zajišťuje zpracování určitých dat, má povinnost zajistit získané osobní informace před možným poškozením, ztrátou, zničením nebo neoprávněným zpracováním. Správce nebo zpracovatel dat by měl také hodnotit potenciální rizika, která hrozí a nehrozí. Tím se míní, že informační systémy a technický stav by měly být pod kontrolou (Nulíček a kolektiv, 2018, s.181-185).

Organizace by měla být také připravena na možná bezpečnostní ohrožení získaných osobních dat, jako je například kybernetický útok, a měla by mít v místě připravené bezpečnostní postupy pro takové situace. Mělo by tam existovat také odpovědné pracoviště, které bude zodpovědné za bezpečnost osobních dat (Nezmar, 2017, s. 74-80).

Princip odpovědnosti

Poslední princip vypovídá o tom, že správce nebo zpracovatel osobních údajů má povinnost dodržovat stanovené zásady a udržovat je v souladu. Je zodpovědný za zajištění dodržování principů zpracování osobních údajů, jak interně, tak u externích zpracovatelů. Ochrana osobních údajů by měla být aktivní, s implementací systémů ochrany, dokumentací a prevencí před problémy (Nezmar, 2017, s. 81-83).

Výše uvedené principy se týkají správy a zpracování osobních údajů vzdělávací institucí a základních práv subjektů, které na instituci vznikají v souvislosti s uchováváním jejich osobních údajů. Jedná se konkrétně o (Obecného nařízení o ochraně osobních údajů (2016/679/EU)):

- právo na to, být informován,
- právo volného přístupu ke svým osobním údajům,
- právo na opravu svých uvedených údajů,
- právo na vymazání svých osobních údajů (tzv. právo být zapomenut),
- právo na to, zamezit nechtěnému zpracování svých osobních dat,
- právo na to, aby mé osobní údaje byly přenositelné,
- právo na to, vznést námitku,
- právo na to, nebýt předmětem automatizovaného rozhodnutí.

2.2 Únik osobních dat

Bezpečnostní rizika, která by mohla potenciálně ohrozit bezpečnost osobních údajů, existuje v současné době nespočetně mnoho. V digitálním věku se nejedná o otázku zda, ale spíše kdy se někdo pokusí poškodit, znehodnotit nebo dokonce odcizit a následně zneužít osobní data. V tomto době vyspělé digitální éry, kdy existuje množství virtuálních úložišť, vzdálených přístupů a složitých IT struktur, je riziko útoku nebo pokusu o útok na bezpečnost dat velmi vysoké. Představa, že školní instituce jsou z tohoto rizika vyloučeny, je bezesporu naivní. Nicméně, dobrou zprávou je, že v současné době existují opatření, která umožňují předem připravit se na tato bezpečnostní rizika a minimalizovat tak jejich potenciálně škodlivé dopady. Školní instituce by měly aktivně investovat do bezpečnostních opatření a strategií, které zahrnují školení zaměstnanců, aktualizaci softwaru, pravidelnou

zálohování dat a silná hesla, důkladné monitorování sítě a přístupových bodů, a vytváření důvěryhodných firemních politik pro správu dat.

Prevence a vzdělávání jsou zásadními pilíři při minimalizaci bezpečnostních rizik. Zaměstnanci a studenti by měli být informováni o nejnovějších hrozbách a rizicích, jako jsou phishingové útoky, malware, ransomware a sociální inženýrství. Tím, že budou mít dostatečné povědomí o těchto rizicích a budou rozpoznávat podezřelé situace, mohou předcházet útokům a snížit riziko úniku nebo zneužití osobních dat.

Kromě toho je důležité, aby školní instituce spolupracovaly s odborníky na kybernetickou bezpečnost a průmyslovými partnery, kteří mohou poskytnout odborné znalosti a pomoc při implementaci bezpečnostních opatření. To zahrnuje pravidelnou aktualizaci softwaru a hardwaru, zajištění firewallů a antivirové ochrany, šifrování dat, správu přístupových práv a aktivní sledování a detekci podezřelých aktivit v síti. Důležitou součástí přípravy na bezpečnostní rizika je také vytvoření plánu pro případ havárie a obnovu dat, který umožní rychlé zotavení v případě útoku nebo jiného incidentu.

Dalším klíčovým prvkem je dodržování přísných standardů ochrany osobních údajů a legislativy. Školní instituce by měly být obeznámeny s příslušnými zákony a nařízeními, jako je například GDPR (Nařízení o ochraně osobních údajů) v Evropské unii, a měly by se řídit jejich pokyny. To zahrnuje například správné zpracování, uchovávání a přenos osobních údajů, zajištění souhlasu s dotčenými osobami a povinnost rychle informovat o případném úniku dat. Bezpečnostní rizika nejsou statická, ale neustále se vyvíjejí. Je proto důležité, aby školní instituce udržovaly si povědomí o aktuálních hrozbách a průběžně aktualizovaly své bezpečnostní opatření a strategie. To zahrnuje pravidelné audity a testování zranitelností, aby bylo možné odhalit případné slabiny a řešit je předtím, než se stanou vstupní branou pro útočníky. Celkově lze říci, že bezpečnost osobních údajů je v dnešní digitální době stále větší výzvou. Avšak s odpovídající přípravou, investicemi do bezpečnostní infrastruktury a neustálým povědomím o rizicích je možné minimalizovat škodlivé dopady bezpečnostních incidentů. Školní instituce mají zodpovědnost chránit osobní data svých zaměstnanců, studentů a rodičů, a proto by měly věnovat dostatečnou pozornost bezpečnosti a přijmout opatření k minimalizaci rizik spojených s únikem nebo zneužitím těchto dat.

Je však dobré si předem uvědomit, že ne všechny bezpečnostní incidenty, ke kterým dojde, je možné ihned označit za únik osobních dat nebo za pokus tento útok spáchat. Nařízení GDPR pod tímto aktem konkrétně chápe „*jakýkoliv incident, který vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí či zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů*.“ (Obecného nařízení o ochraně osobních údajů (2016/679/EU)).

Incidenty ohrožující bezpečnost osobních údajů mohou mít různé příčiny a původce. Jedním z možných vysvětlení je úmyslný a cílený hackerský útok, při kterém se útočníci snaží získat neoprávněný přístup k školním databázím obsahujícím osobní údaje. Avšak není vyloučena ani možnost, že ke ztrátě nebo úniku dat může dojít náhodou nebo v důsledku lidského selhání. Jako příklad může sloužit situace, kdy zaměstnanec omylem zapomene svůj pracovní notebook na veřejném místě. Pokud má notebook zapnutý vzdálený přístup do školní databáze s osobními údaji, může dojít k ohrožení bezpečnosti dat v případě, že se notebook dostane do nesprávných rukou. Navíc není nutné, aby únik dat byl spojen s přímým proniknutím do digitálního systému ochrany osobních údajů. Může se jednat o porušení zabezpečení fyzických záznamů obsahujících citlivé informace. Tyto záznamy mohou být poškozeny, ztraceny, zničeny nebo odcizeny, čímž se vystavují riziku neoprávněného přístupu k osobním údajům. Narušení zabezpečení dat může nastat i náhodně, například v důsledku aktivit škodlivého softwaru, který se dostane do systému nebo zařízení. Tento druh malwaru, známý jako virus, může způsobit změny, poškození, zašifrování nebo úpravy osobních údajů, což má za následek ohrožení jejich bezpečnosti. Je zřejmé, že incidenty ohrožující bezpečnost osobních údajů ve školství mohou mít různé příčiny a formy. Ať už jde o cílené útoky, lidské chyby, fyzické porušení zabezpečení nebo náhodné narušení systému, je důležité, aby školní instituce měly v místě odpovídající ochranná opatření a postupy, které minimalizují riziko úniku a zneužití osobních údajů. (Škorničková, 2018).

Důvod uchovávání osobních údajů a jejich účely sehrávají klíčovou roli při posuzování bezpečnostních rizik. Důležitým faktorem je také povaha těchto údajů, zda se jedná o citlivé informace, které vyžadují zvláštní ochranu, například v případě zdravotních záznamů pacientů v nemocnicích. V případech, kdy jsou zpracovávány citlivé osobní údaje, může i zdánlivě banální událost, jako je výpadek elektřiny, představovat značné bezpečnostní riziko. V případě výpadku elektřiny může dojít k přerušení přístupu k systémům, což znamená, že údaje budou dočasně nedostupné. V nemocnicích by to mohlo mít závažné

následky, protože pacienti nebudou moci být diagnostikováni, léčeni nebo podstoupit operace, protože zdravotnický personál nebude mít přístup k jejich záznamům. Na druhou stranu pro jiné instituce, jako jsou například školské instituce, by výpadek elektřiny a dočasná nepřístupnost dat nemusely představovat tak závažný problém. I když by mohl nastat dočasný výpadek přístupu k informacím, neovlivnil by to okamžité fungování a běžné operace školy. Je tedy zřejmé, že v závislosti na důvodech uchovávání osobních údajů a jejich citlivosti se rizika spojená s výpadkem elektřiny nebo dočasnou nepřístupností dat mohou lišit. Je důležité, aby instituce, které zpracovávají osobní údaje, měly v místě odpovídající záložní systémy, plán obnovy po havárii a další bezpečnostní opatření, která minimalizují rizika a zajišťují, že v případě výpadku bude přístup k důležitým údajům co nejrychleji obnoven a případné dopady budou minimalizovány. (Škorničková, 2018).

Každá situace, která může ohrozit bezpečnost umístěných osobních údajů, vyžaduje pečlivé zhodnocení a odpovídající opatření. V souladu s právními předpisy je každý správce a zpracovatel osobních údajů povinen okamžitě informovat Úřad pro ochranu osobních údajů o jakémkoli incidentu, který může mít vliv na osobní údaje. Je důležité, aby tato oznámení byla provedena bez zbytečného odkladu, ideálně do 72 hodin od odhalení události. Nicméně platí pravidlo, že čím dříve je incident nahlášen, tím lépe. Oznámení takových událostí Úřadu pro ochranu osobních údajů slouží k zajištění dodržování předpisů a ochrany práv a soukromí jednotlivců, jejichž osobní údaje byly ohroženy. Správci a zpracovatelé osobních údajů mají povinnost transparentně informovat o incidentech a spolupracovat s příslušnými úřady při vyšetřování a minimalizaci případných negativních dopadů. Tato povinnost ohlášení incidentů pomáhá zajišťovat vysokou úroveň ochrany osobních údajů a rychlou reakci na bezpečnostní problémy. Při dodržování této povinnosti se zajišťuje, že případné škody budou minimalizovány a další opatření pro ochranu osobních údajů budou přijata včas. Je zásadní, aby správci a zpracovatelé osobních údajů věnovali zvýšenou pozornost sledování a hlášení bezpečnostních incidentů, aby mohli co nejrychleji reagovat na potenciální rizika a zajistit ochranu osobních údajů a soukromí jednotlivců. (Škorničková, 2018).

Podle pravidel stanovených v GDPR (Obecné nařízení o ochraně osobních údajů) je rozhodujícím okamžikem ten moment, kdy správce nebo zpracovatel osobních dat zjistí, že existuje důvodný důvod k obavám o porušení zabezpečení osobních údajů, které by mohly být potencionálně znehodnoceny, pozměněny nebo odcizeny. Vyhodnocení, zda se jedná o

skutečné porušení závisí na konkrétním případu a situaci, která ho provází. Rozdíl je například mezi propracovaným a plánovaným hackerským útokem a ztrátou zaměstnancova notebooku na vlakovém nádraží. Přestože každý incident vyžaduje individuální posouzení, vznikne-li jakákoli bezpečnostní hrozba, je vždy vhodné kontaktovat Úřad pro ochranu osobních údajů. Díky GDPR jsou správci a zpracovatelé osobních údajů povinni přijímat opatření k identifikaci a řešení bezpečnostních incidentů. Jejich úkolem je zajistit, že jakékoliv porušení zabezpečení je řádně zhodnoceno a informováno příslušné úřady. Spolupráce s Úřadem pro ochranu osobních údajů je klíčová pro posouzení rozsahu a případných dopadů bezpečnostního incidentu, a to nezávisle na subjektivním hodnocení v daném okamžiku. Kontaktování Úřadu pro ochranu osobních údajů při vzniku bezpečnostní hrozby je důležité, protože takový krok zajišťuje řádné dodržování právních předpisů, ochranu práv a soukromí jednotlivců a případnou podporu při vyšetřování a řešení incidentu. Je tedy v zájmu správců a zpracovatelů osobních údajů jednat rychle a odpovědně, aby minimalizovali případné škody a dodrželi požadavky GDPR na hlášení bezpečnostních incidentů. (Škorničková, 2018).

Pokud je identifikovaný incident vyhodnocen jako bezpečnostní hrozba, od tohoto okamžiku začíná plynout 72hodinová lhůta, během které je nezbytné provést posouzení potenciálních dopadů tohoto incidentu. Úspěch této operace závisí na řadě faktorů, včetně interních mechanismů nastavených danou institucí a schopností a zkušenostech zaměstnanců. Zaměstnanci, kteří jsou odpovědni za bezpečnostní systém ochrany osobních dat, jsou pravděpodobně mezi prvními, kteří se o bezpečnostní hrozbě dozvědí. Z tohoto důvodu je nezbytné, aby pověřencem pro ochranu osobních údajů byl zaměstnanec s odpovídajícím odborným školením, který je schopen rozpoznat útok nebo hrozbu a ví, jak postupovat dále (komu incident nahlásit, jaké faktory vyhodnocovat atd.). Kvalifikovaný pověřenec pro ochranu osobních údajů je klíčovou osobou při řízení bezpečnostních hrozeb. Měl by mít dostatečné znalosti a dovednosti v oblasti kybernetické bezpečnosti a ochrany osobních údajů, aby byl schopen identifikovat příznaky útoku a provést potřebné kroky k minimalizaci škod. Jejich role zahrnuje monitorování, detekci a rychlou reakci na bezpečnostní incidenty, jakož i znalost interních postupů a protokolů pro řešení takových situací. Při správném vykonávání role pověřence je tedy klíčové, aby zaměstnanec pověřený ochranou osobních údajů měl odpovídající odbornou přípravu a neustále se zdokonaloval ve svých schopnostech. Tímto způsobem může identifikovat a reagovat na bezpečnostní incidenty,

provádět vyhodnocování a informovat příslušné subjekty o jejich povaze a rozsahu. (Škorničková, 2018).

Ohlašovací povinnost úřadům však nevzniká vždy. A to konkrétně za situací, kdy je incident vyhodnocen jako porušení bez pravděpodobných rizik vůči právům a svobodám fyzických osob (Škorničková, 2018).

2.3 Role pověřenců pro ochranu osobních údajů

Veřejné vzdělávací instituce jsou významnými zpracovateli osobních údajů, neboť shromažďují a zpracovávají rozsáhlé množství informací o svých studentech, učitelích, zaměstnancích a dalších subjektech. V souladu s Nařízením GDPR jsou tyto instituce povinny jmenovat pověřence GDPR, který zastává klíčovou roli při zajišťování souladu s předpisy ochrany osobních údajů. Pověřenec pro ochranu osobních údajů je odborník na ochranu osobních údajů, který je odpovědný za dohled nad dodržováním zásad ochrany osobních údajů ve vzdělávací instituci. Jeho úkolem je zajistit, že instituce splňuje všechny právní povinnosti v oblasti ochrany osobních údajů a že jsou zavedena vhodná technická a organizační opatření pro ochranu osobních údajů. Pověřenec pro ochranu osobních údajů má za úkol poskytovat informace a rady týkající se ochrany osobních údajů, monitorovat dodržování předpisů GDPR, spolupracovat s dozorovými orgány a v případě potřeby vykonávat audity a kontroly v rámci instituce. Pověřenec je také kontaktní osobou pro dotazy a stížnosti týkající se ochrany osobních údajů. Jmenování pověřence pro ochranu osobních údajů je důležitým opatřením, které pomáhá vzdělávacím institucím plnit své závazky v oblasti ochrany osobních údajů. Pověřenec zajišťuje, že v instituci existuje odborná osoba, která má přehled o právních předpisech a nejlepších postupech v oblasti ochrany osobních údajů a aktivně přispívá k minimalizaci rizik spojených se zpracováním osobních údajů.

Pověřenec pro ochranu osobních údajů, jak již bylo zmíněno, je klíčovou postavou ve zajištění souladu s předpisy ochrany osobních údajů. Je to nestranný a nezávislý subjekt, který přebírá určité povinnosti a odpovědnosti od instituce, orgánu nebo podniku týkající se zpracování a uchovávání osobních údajů. Pověřenec může být interní zaměstnanec dané instituce nebo podniku, který je speciálně vyškolen a pověřen touto funkcí. Tento zaměstnanec se stává odborníkem na ochranu osobních údajů a je odpovědný za dohled nad jejich správným zpracováním. Jeho úkolem je zabezpečit soulad s právními předpisy,

vyhodnocovat rizika a implementovat vhodná opatření pro ochranu osobních údajů. Alternativně může být pověřencem zcela nezávislý externí pracovník, který spolupracuje s institucí, orgánem nebo podnikem na základě smlouvy. Tento externí pověřenec přináší nezávislý pohled a odborné znalosti z oblasti ochrany osobních údajů. Jeho role je stejně důležitá jako role interního pověřence, a to ve smyslu poskytování odborných rad, monitorování dodržování předpisů a zajištění souladu s předpisy ochrany osobních údajů. Přítomnost pověřence pro ochranu osobních údajů, ať už interního nebo externího, je zásadní pro zajištění řádného a odpovídajícího zpracování osobních údajů. Jejich nezávislost a odbornost jsou klíčové pro minimalizaci rizik spojených se zpracováním a uchováváním osobních údajů, a přispívají k vytvoření důvěry veřejnosti v ochranu jejich soukromí a práv (Nulíček a kolektiv, 2018, s. 365-367).

Vzdělávací instituce mají důležitou povinnost zajistit ochranu osobních údajů svých svěřenců. Jedním z klíčových kroků k dosažení tohoto cíle je zapojení pověřence pro ochranu osobních údajů do procesu zpracování těchto dat. Tímto způsobem je zajištěna odborná a specializovaná péče o ochranu osobních údajů ve vzdělávací instituci. Instituce jsou povinny zajistit, že pověřenec pro ochranu osobních údajů je zapojen co nejdříve do všech činností týkajících se zpracování osobních údajů svých svěřenců. To zahrnuje jeho účast při vytváření interních postupů, poskytování odborných rad a dohled nad dodržováním právních předpisů v oblasti ochrany osobních údajů. Dále je pro vzdělávací instituci povinností zveřejnit kontaktní údaje pověřence pro ochranu osobních údajů na svých webových stránkách. Tímto způsobem je umožněno svěřencům, rodičům či zákonným zástupcům a dalším zúčastněným stranám, aby se mohli obrátit na pověřence s dotazy, podněty nebo obavami týkajícími se ochrany jejich osobních údajů. Tím se posiluje transparentnost a důvěra veřejnosti v rámci procesu zpracování osobních údajů ve vzdělávací instituci. Zapojení pověřence pro ochranu osobních údajů a zveřejnění jeho kontaktu na webových stránkách vzdělávací instituce představuje důležitý krok k zajištění odpovídající ochrany osobních údajů a respektování práv svěřenců. Tím je umožněno řádné vyřizování dotazů a případných stížností a poskytuje se jasná cesta pro komunikaci a řešení otázek souvisejících s ochranou osobních údajů ve vzdělávacím prostředí.

Pověřenec má nejen ve vzdělávacích institucích za úkol splnit alespoň minimální povinné úkoly, které mu jsou GDPR uloženy. Mezi ně konkrétně patří (Nulíček a kolektiv, 2018, s. 360-365):

- poskytovat informace správcům a zpracovatelům osobních údajů (respektive vzdělávacím institucím, kterými byli do své funkce jmenováni),
- sledovat a dodržovat soulad s nařízeními a dalšími předpisy,
- poskytovat poradenskou činnost, a to jak svěřencům, tak jejich zákonným zástupcům,
- posuzovat stupeň ochrany zpracovávaných a ukládaných osobních údajů,
- spolupracovat s dozorovým úřadem, pro který představuje kontaktní místo.

Většina vzdělávacích institucí na svých webových stránkách mimo kontaktu na pověřence pro ochranu osobních údajů také uvádí, že na tuto zodpovědnou osobu se mají zákonní zástupci nebo svěřenci obracet s jakýmikoliv dotazy. Dále mají být pověřenci zasílány podněty a požadavky, které se týkají uplatnění práv týkajících se přímo osobních údajů svěřenců nebo jejich zástupců, které jsou používány v rámci některé agendy ve škole, a to zejména, pokud se nechtějí obrátit přímo na zástupce školy.

Pověřenec pro ochranu osobních údajů hraje klíčovou roli při vyhodnocování dotazů, požadavků a podnětů od dotazatelů. Jeho úkolem je pečlivě a odborně posoudit tyto případy a následně je předat správci osobních údajů, tj. vzdělávací instituci, spolu s doporučením ohledně jejich řešení. Pověřenec může také poskytnout dotazatelům základní informace a konzultaci, které jim pomohou lépe porozumět jejich právům a ochraně osobních údajů. Je důležité zdůraznit, že pověřenec je vázán mlčenlivostí a dodržuje důvěrnost všech informací týkajících se dotazů, stížností nebo podnětů, které obdrží. Tím je zajištěna ochrana soukromí a důvěrnosti dotazatelů. Je však důležité poznamenat, že odpovědnost za vyřízení dotazů, podnětů, námitek a požadavků leží výhradně na správci osobních údajů, tedy na vzdělávací instituci a jejím vedení. Pověřenec slouží jako odborný poradce a prostředník, který předává informace a doporučení správci, avšak konečné rozhodnutí o jejich vyřízení je v pravomoci správce. Tímto způsobem je zajištěno, že dotazatelé mají k dispozici mechanismus pro komunikaci a řešení otázek týkajících se ochrany osobních údajů ve vzdělávací instituci. Pověřenec vystupuje jako prostředník, který pomáhá zajistit, že dotazy jsou řádně vyřízeny a práva jednotlivců jsou respektována v souladu s platnými právními předpisy.

Ve článku 38 Obecného nařízení o ochraně osobních údajů (2016/679/EU) je stanoveno, že „*správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem*

nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele."

Pověřenec pro ochranu osobních údajů, zejména pokud se jedná o externího pracovníka, není obvyklým zaměstnancem vzdělávací instituce, která ho najala. Jeho role je zcela odlišná. Správce a zpracovatel osobních údajů, konkrétně škola a její ředitel, nemají pravomoc zadávat pověřenci své úkoly nebo rozhodnutí. Vzdělávací instituce nemá nad pověřencem žádnou moc a nemůže ho propustit. Pověřenec je angažován s cílem plnit své povinnosti v souladu s Nařízením GDPR. Samozřejmě, pokud by nedodržoval své povinnosti, může být sankcionován. I pověřenec, kterého najal ředitel školy, musí splňovat základní povinnosti a dodržovat interní předpisy školy. Tímto způsobem se zajistí, že pověřenec pro ochranu osobních údajů má svou nezávislost a že jeho rozhodnutí a činnosti jsou řízeny Nařízením GDPR a vnitřními pravidly ochrany osobních údajů. Pověřenec slouží jako garant integrity a dodržování práv jednotlivců týkajících se jejich osobních údajů ve vzdělávací instituci. (Navrátil a kolektiv, 2018, s. 241)

Pokud pověřenec pro ochranu osobních údajů není externí pracovník, ale zaměstnanec vzdělávací instituce, který má navíc nadstandardní povinnosti, pak se jedná o klasického zaměstnance školy. Avšak ředitel školy nesmí zasahovat do záležitostí týkajících se ochrany osobních údajů. Nemá pravomoc přikazovat pověřenci, jak má vykonávat svou práci, pokud se týká správy osobních údajů. Pokud však zaměstnanec nesplňuje své povinnosti, může být sankcionován nebo propuštěn. Navíc, pokud pověřencem je osoba, která ve škole zastává i jiné funkce, musí se zajistit, aby tato pozice nebyla ve střetu zájmů s ochranou dat. Je důležité, aby pověřenec měl nezávislou pozici a mohl svobodně vykonávat své povinnosti v souladu s právními předpisy o ochraně osobních údajů. Ředitel školy by měl uznávat a respektovat rozhodnutí a doporučení pověřence v oblasti ochrany osobních údajů a zajistit mu nezbytné prostředky a podporu k plnění jeho úkolů. Tím se zajišťuje důvěryhodnost a účinnost procesu ochrany osobních údajů ve vzdělávací instituci. (Navrátil a kolektiv, 2018, s. 258-261).

3 Metodologie

V rámci výzkumné části bakalářské práce byl realizován kvantitativní výzkum v podobě tzv. dotazníkového šetření. Dotazníkové šetření si kladlo za cíl konkrétně zjistit, jakým způsobem vedení současných českých škol zajišťuje ochranu osobních údajů svých svěřenců a zaměstnanců. Zjištěné informace byly vyhodnocovány prostřednictvím předem stanovených výzkumných otázek, které konkrétně zněly:

1. Jakým způsobem vedení školy chrání osobní údaje ve škole?

2. Proč je vhodný k delegování ochrany osobních údajů pověřenec GDPR?

3. V jakých nejčastějších případech dochází k únikům osobních údajů ze škol?

Účelem dotazníkového průzkumu bylo zjištění, jaké metody vedení škol uplatňuje k zajištění ochrany osobních údajů svých studentů, proč je podle školního názoru důležitá role pověřence pro ochranu osobních dat a jestli a za jakých podmínek se v rámci jejich instituce vyskytl incident s únikem osobních údajů.

3.1 Výzkumný cíl

„*Stanovení cíle práce je nejdůležitějším krokem při tvorbě jakéhokoli textu, správně stanovený cíl provede autora bezpečně všemi úskalími tvorby, umožní mu správně zvolit metodologický přístup, položit správné výzkumné otázky či hypotézy, dobře ho nasměruje k vhodným výzkumným nástrojům a celkově je kormidlem, které řídí celou práci.*“ (Svobodová, 2020)

Cíl práce byl stanoven na zpracovaní návrh řešení ochrany osobních údajů ve školách, včetně vypořádání se s možným únikem dat.

3.2 Popis výzkumného vzorku

V důsledku toho byli pro získání informací osloveni všichni ředitelé jednotlivých vzdělávacích zařízení, tj. všech základních škol v Ústeckém kraji. Ti představují správce a zpracovatele osobních dat svých studentů, a toto oslovení bylo autorstvím této bakalářské práce. prostřednictvím e-mailové komunikace bylo kontaktováno všech 287 ředitelů

základních škol v Ústeckém kraji. V e-mailu bylo jasně vysvětleno, o čem je výzkum a dotazníkové šetření, k jakým účelům budou informace zpracovány a co se bude zkoumat. Bylo zdůrazněno, jak důležité jsou výsledky tohoto šetření, které by mohly přispět ke zlepšení bezpečnosti ochrany osobních dat v českých základních školách a osvětlit celou tuto problematiku pro nezasvěcené čtenáře. Potenciálním respondentům bylo jasně sděleno, že dotazníkové šetření probíhá zcela anonymně a ředitelé škol nemusí uvádět žádné osobní údaje o sobě ani o své instituci.

3.3 Popis sběru dat

Průzkum proběhl v období mezi květnem a červnem roku 2023. Respondentům bylo poskytnuto 17 dní k vyplnění dotazníkového šetření a za jejich odpovědi a čas bylo vyjádřeno poděkování. Dotazník byl vytvořen na online platformě survio.com, která je specializována na elektronické dotazníky. Očekávaná doba potřebná k vyplnění dotazníku byla přibližně 5 minut.

Dotazníkové šetření bylo koncipováno jako soubor 11 výzkumných otázek, které byly rozděleny do dvou částí. V první části se zaměřovaly spíše na obecné aspekty (známé také jako vstupní data), zatímco ve druhé části se stávaly specifičtějšími a subjektivnějšími (označovanými také jako výstupní data).

Vstupní data se zabývala širším kontextem a zahrnovala témata, která předcházela konkrétnímu předmětu zkoumání. Tyto otázky sloužily k získání obecného povědomí a informací o dané problematice. Naopak výstupní data se soustředila na detailnější a individuální aspekty, s cílem získat subjektivní názory a zkušenosti respondentů.

Tímto přístupem bylo dosaženo postupného prohloubení výzkumu a umožněno získání širšího pohledu na zkoumanou problematiku. Vstupní data poskytla základní rámec a kontext, na němž byla stavěna výstupní část dotazníku, která se pak zaměřovala na konkrétní a individuální aspekty zájmu.

3.4 Popis analýzy dat

Po sběru dat byla získaná data zpracována a analyzována pomocí programu Microsoft Excel. Dotazníkové šetření obsahovalo jednotlivé otázky, které byly formulovány s cílem

minimalizovat zkreslení výsledků. Odpovědi na každou otázku byly následně vyhodnoceny a graficky znázorněny.

Po získání dat proběhla jejich strukturování a organizace v programu Microsoft Excel, který poskytuje nástroje pro analýzu a manipulaci s daty. Získané odpovědi byly systematicky zpracovány a převedeny do tabulkového formátu, aby bylo možné provést další analýzu.

Vyhodnocení dat zahrnovalo různé techniky a metody výzkumné analýzy. Kromě tabulkových dat bylo také využito grafického znázornění, což umožnilo vizuálně prezentovat výsledky a lépe porozumět vzorcům či trendům, které v datech byly identifikovány. Tímto grafickým znázorněním byly výsledky přehledně a srozumitelně prezentovány, což usnadnilo interpretaci dat a závěrů z výzkumu.

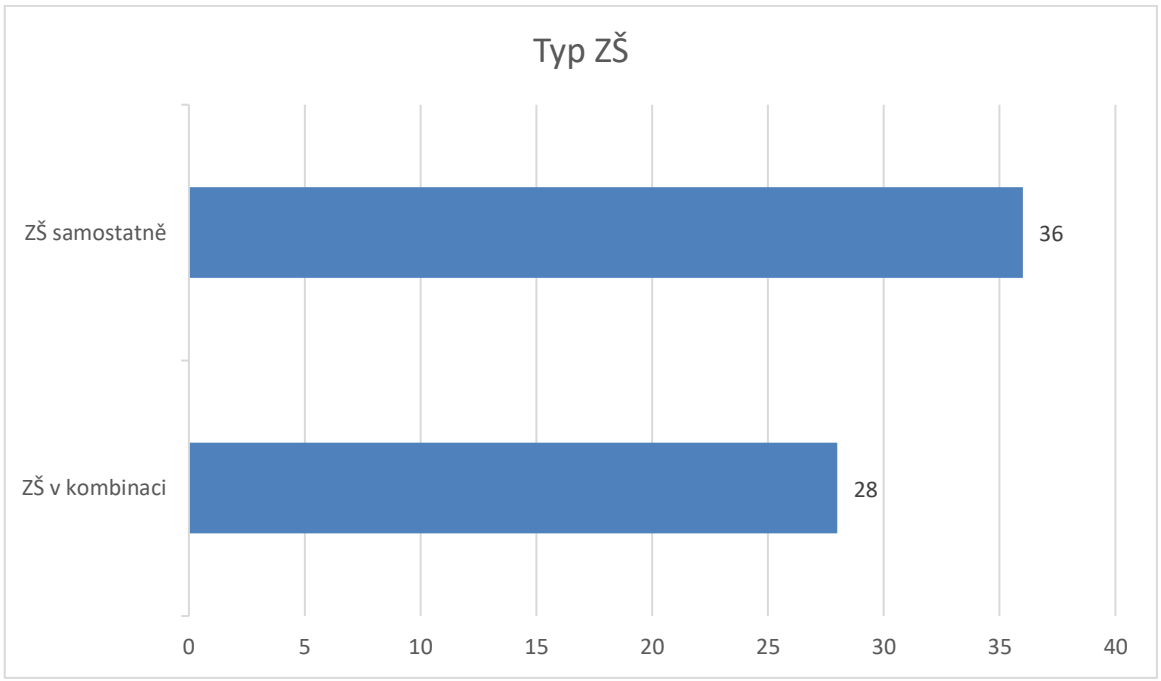
Během průzkumu bylo osloveno celkem 287 respondentů, tedy všem ředitelům základních škol v Ústeckém kraji. Z těchto respondentů 64 vyplnilo dotazník v plném rozsahu, což odpovídá účasti 23 % ze všech oslovených subjektů. Tato návratnost ukazuje na dobré zapojení respondentů a zájem o zkoumanou problematiku.

Průměrná doba vyplnění dotazníku byla stanovena na 4,2 minuty. Tento údaj vypovídá o očekávaném časovém rámci, který respondentům zabralo vyplnění všech otázek. Byla předpokládána dostatečná efektivita a stručnost dotazníku, což přispělo k relativně krátkému časovému nároku na vyplnění.

4 Výsledky výzkumu

1. Otázka: V jakém kombinaci ZŠ pracujete?

Graf 1: Typ ZŠ

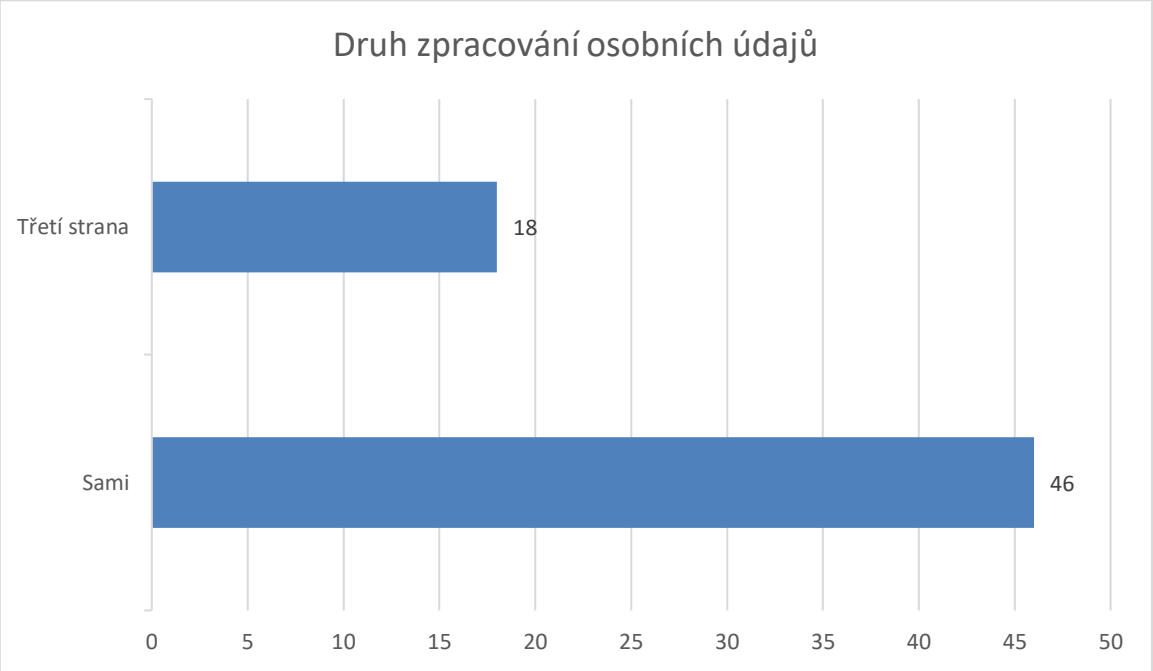


Zdroj: Vlastní zpracování

V rámci první otázky byly subjekty dotazovány, jaký typ základní školy spravují. Jak lze vidět z výsledků otázky, nejvíce subjektů, více než polovina (36 z 64) spravuje samostatnou ZŠ. V ostatních případech (28 z 64) šlo o kombinace ZŠ s dalšími druhy škol/zařízení.

2. Otázka: Zpracováváte si a chráníte osobní údaje svých svěřenců sami nebo využíváte třetí stranu?

Graf 2: Druh zpracování osobních údajů



Zdroj: Vlastní zpracování

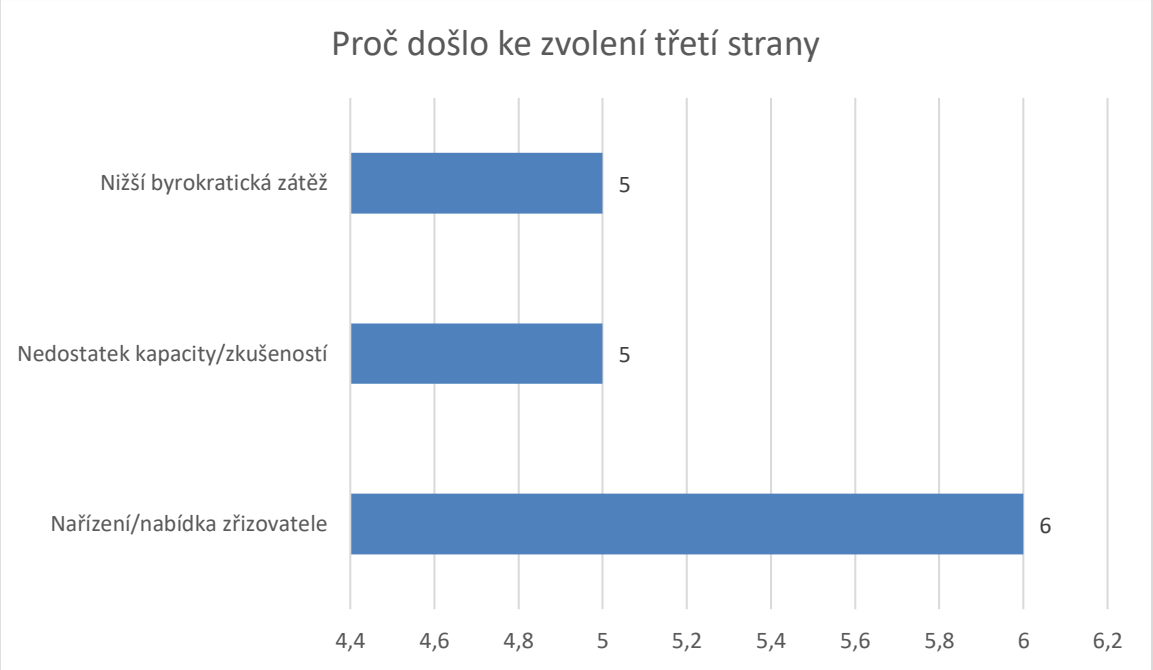
Ve druhé otázce bylo zkoumáno, zda při zpracování osobních údajů využívají školy služeb třetích stran, jako jsou specializované společnosti, nebo zda zpracování dat provádějí školy samy. Cílem tohoto dotazu bylo zjistit, zda školy outsourcují část zpracování dat a svěřují je externím specialistům, nebo zda mají vlastní interní procesy pro zpracování a ochranu osobních údajů svých svěřenců. Tímto se získávala informace o přístupu škol k zajištění bezpečnosti a soukromí osobních dat ve vztahu k externím subjektům.

Z výsledků plyne, že většina škol si zpracovává osobní údaje svých svěřenců sama. Tyto školy mají vlastní pověřenou osobu, která je odpovědná za správu a ochranu osobních dat. Tímto přístupem si školy udržují kontrolu nad procesem zpracování a zajišťují bezpečnost a důvěrnost osobních údajů. Naopak 18 škol se rozhodlo svěřit zpracování a ochranu dat třetí nezávislé straně. Tímto přístupem si tyto školy umožňují využívat specializované služby a znalosti externích poskytovatelů, kteří mají odborné znalosti v oblasti zpracování dat a

ochrany soukromí. Tento přístup může školám poskytnout větší efektivitu a expertízu v oblasti správy osobních údajů.

3. **Otázka: Z jakého důvodu jste zvolili možnost, nechávat si osobní údaje zpracovávat a chránit třetí nezávislou stranou?**

Graf 3: Důvod zvolení třetí strany



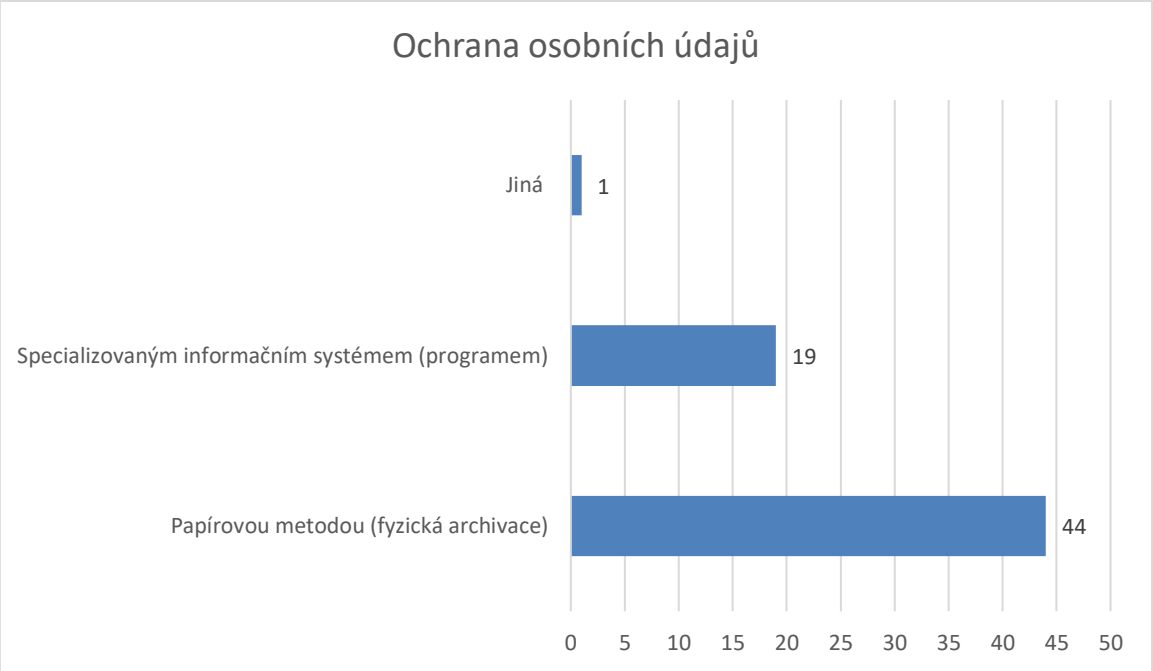
Zdroj: Vlastní zpracování

Třetí otázka měla charakter doplňujícího dotazu, který byl kladen pouze těm subjektům, jež vybraly možnost svěření zpracování a ochrany osobních údajů třetí straně. Tímto termínem se myslí specializovaná společnost, která se specializuje na ochranu a zpracování dat podle směrnice GDPR.

Tato otázka byla tzv. volná, subjekty na ní mohly odpovídat podle svého uvážení, a nebyly jim podsouvány žádné konkrétní odpovědi, ze kterých by si musely zvolit Jak lze vidět v grafu, 6 subjektů uvedlo, že je to nařízení či nabídka zřizovatele. Další významná odpověď (5 respondentů) uvedlo, že k tomuto tématu se necítí být dostatečně zkušení, anebo nemají dostatečnou kapacitu. 5 dalších subjektů uvedlo, že jde o nižší byrokratickou zátěž.

4. Otázka: Jakým způsobem ve Vaší škole dochází k ochraně osobních dat?

Graf 4: Způsob ochrany osobních údajů

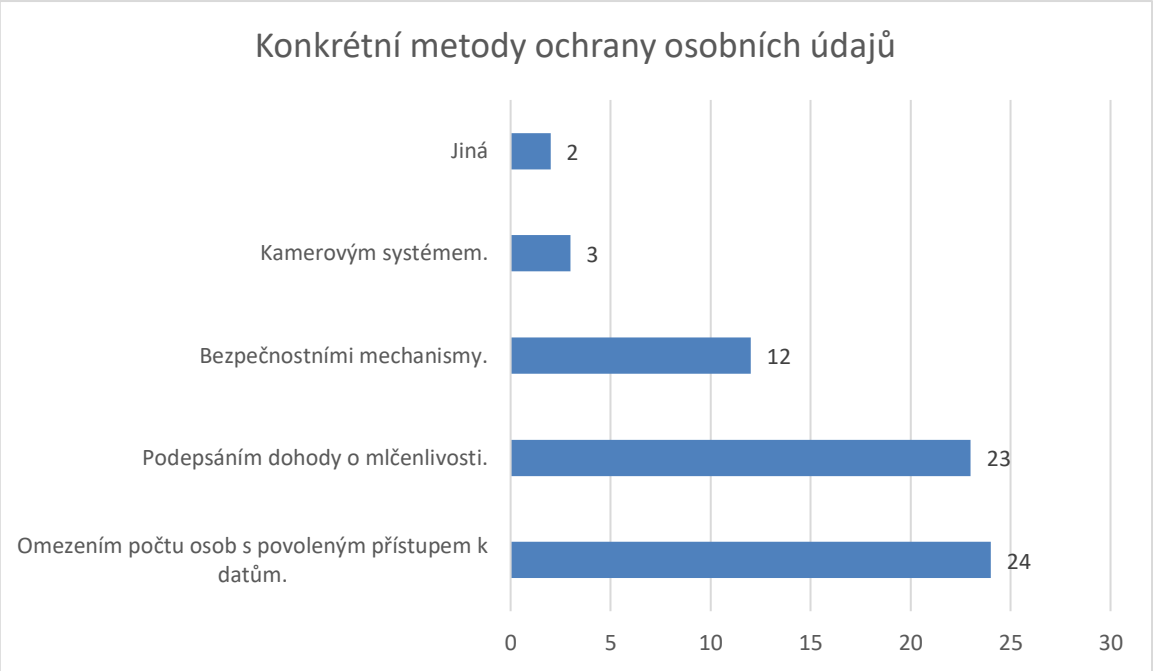


Zdroj: Vlastní zpracování

V rámci čtvrté otázky byla zkoumána konkrétní opatření, která subjekty uplatňují pro ochranu osobních údajů svých svěřenců v rámci jejich instituce. Většina subjektů uvedla, že využívají papírovou metodu (fyzickou archivaci) (44 subjektů). 19 škol využívá k ochraně osobních údajů specializovaný informační systém (program). Pouze jeden respondent odpověděl, že využívá jiný způsob.

5. Otázka: Jakými konkrétními metodami jsou osobní data chráněna?

Graf 5: Metody pro ochranu osobních údajů



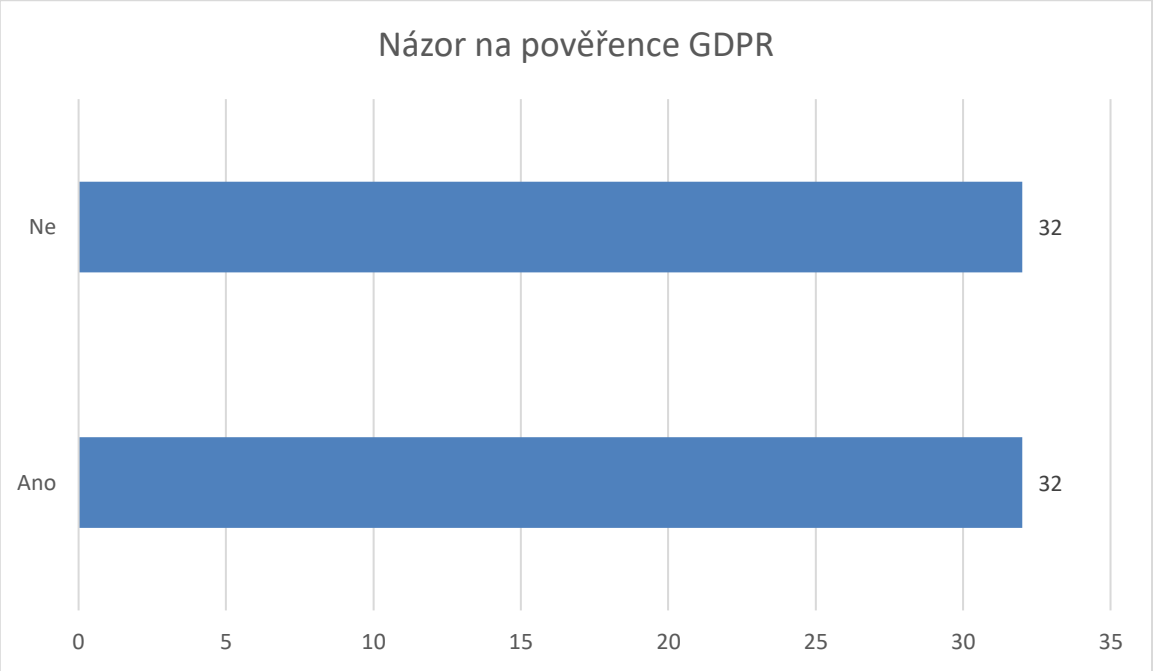
Zdroj: Vlastní zpracování

V rámci páté otázky byly subjekty vyzvány k výběru konkrétních metod, které používají pro ochranu osobních údajů svých svěřenců. Autor této práce si byl vědom toho, že ke čtvrté otázce bude nutné přidat další, doplňující otázku. Cílem bylo získat od subjektů podrobný popis metod, které aktivně uplatňují pro zajištění bezpečnosti citlivých dat.

Jak lze vidět, 24 subjektů uvedlo, že pro ochranu osobních údajů využívá omezení počtu osob s povoleným přístupem k datům. Další četné zastoupení (23 subjektů) využívá některou z podob dohody o mlčenlivosti. Dalších 12 subjektů odpovědělo, že využívají bezpečnostní mechanismy. Subjekty měly na mysli různá zabezpečení, kódování, šifrování a další mechanismy, které je možné využít informačními systémy.

6. **Otázka: Považujete za správné, že ochrana dat ve školství musí být delegována na odpovědnou osobu, tzv. pověřence pro ochranu osobních dat?**

Graf 6: Názor na ustanovení povinnosti funkce pověřence GDPR

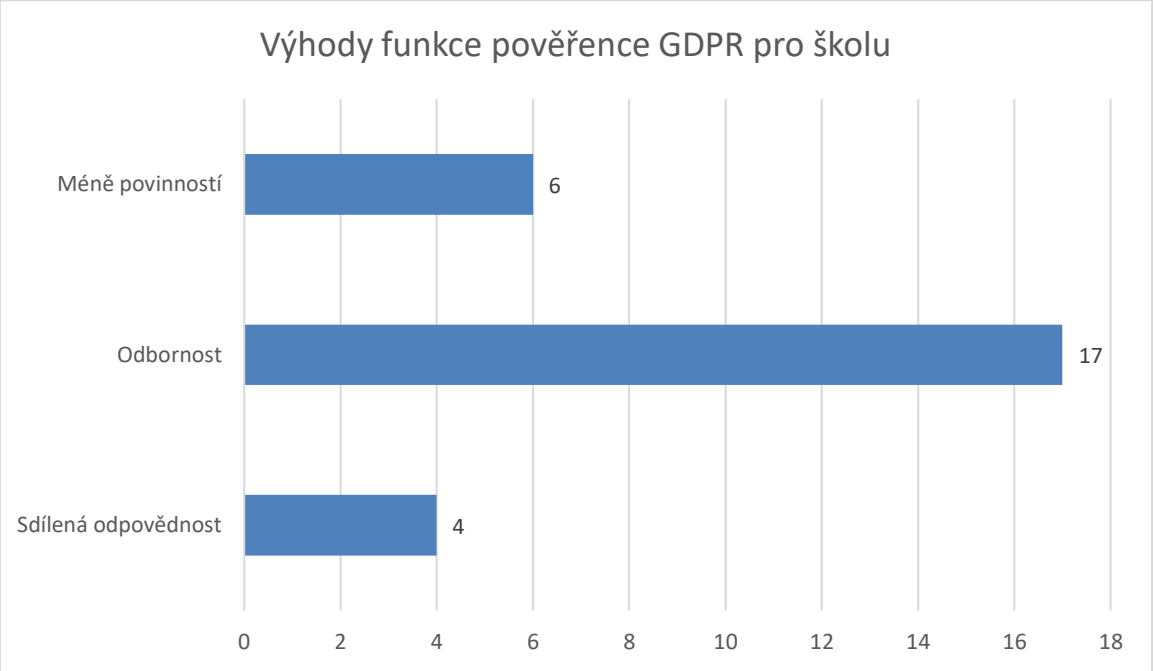


Zdroj: Vlastní zpracování

V rámci šesté otázky byly subjekty vyzváni vyjádřit svůj názor na potřebu pověřence pro ochranu osobních údajů. Jak ukazují výsledky, přesná polovina považuje toto opatření za prospěšné pro ochranu osobních údajů a pravděpodobně i pro dobro vzdělávacích institucí. Druhá polovina subjektů ale vyjádřila nesouhlas s touto funkcí, která byla zavedena Evropskou unií. Z výsledků je patrné, že na tuto otázku není mezi řediteli ZŠ v Ústeckém kraji vyhraněný názor.

7. Otázka: Proč konkrétně je podle Vás funkce pověřence GDPR vhodná/výhodná pro školní instituce?

Graf 7: Výhody funkce pověřence GDPR



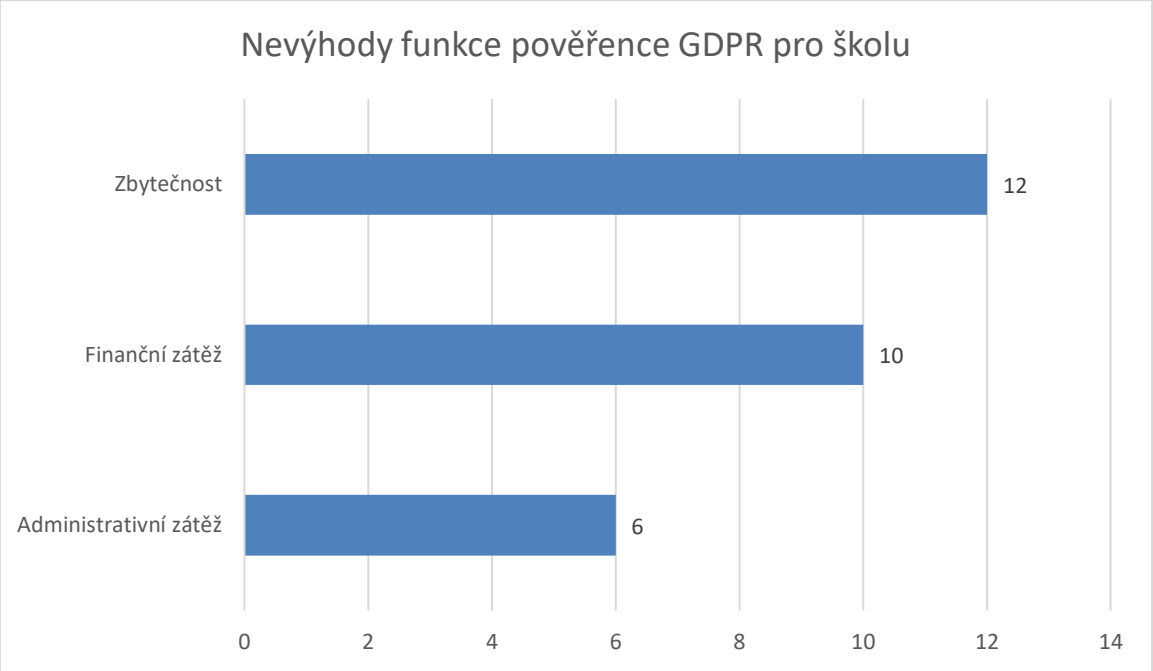
Zdroj: Vlastní zpracování

Sedmá otázka byla doplňující otázkou pro respondenty, kteří v minulé otázce odpověděli, že považují za správné delegaci správy ochrany osobních údajů tzv. pověřencem pro ochranu osobních údajů.

Většina respondentů na tuto otevřeno otázku reagovala tím, že kvitovali odbornost pověřence. Má aktuální informace k tématu a je schopen je ihned implementovat do praxe. Další nemalou skupinou odpovědí bylo, že z toho vyplývá méně povinností pro školu.

8. Otázka: Proč konkrétně je podle Vás funkce pověřence GDPR nevhodná/nevýhodná pro školní instituce?

Graf 8: Nevýhody funkce pověřence GDPR



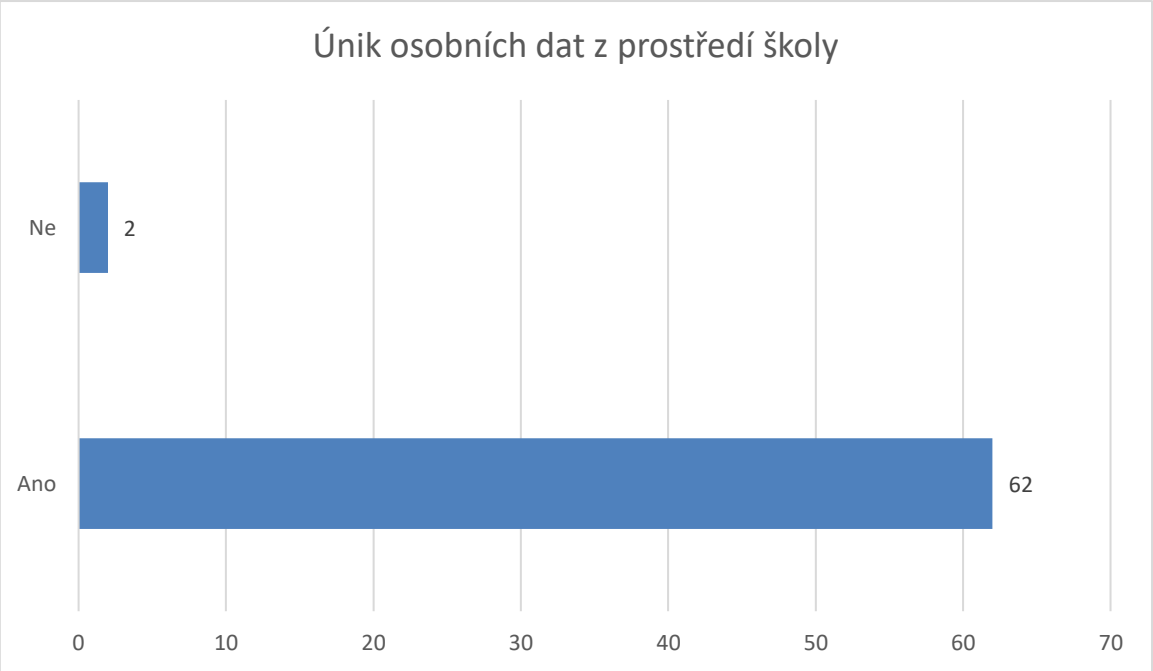
Zdroj: Vlastní zpracování

Otázka 8 byla určena pro ty respondenty, kteří v 6. otázce odpověděli, že nepovažují za správné delegaci správy ochrany osobních údajů tzv. pověřencem pro ochranu osobních údajů.

Zde subjekty ponejvíc uvádějí, že jde o zbytečnou funkci, kde by tuto problematiku uměli řešit sami. Další podstatné zastoupení v odpovědích je finanční zátěž. Dále se pak četně objevovala odpověď, která zmiňovala neúměrnou administrativní zátěž.

9. Otázka: Došlo ve Vaší škole někdy k úniku osobních dat?

Graf 9: Únik osobních dat ze školy



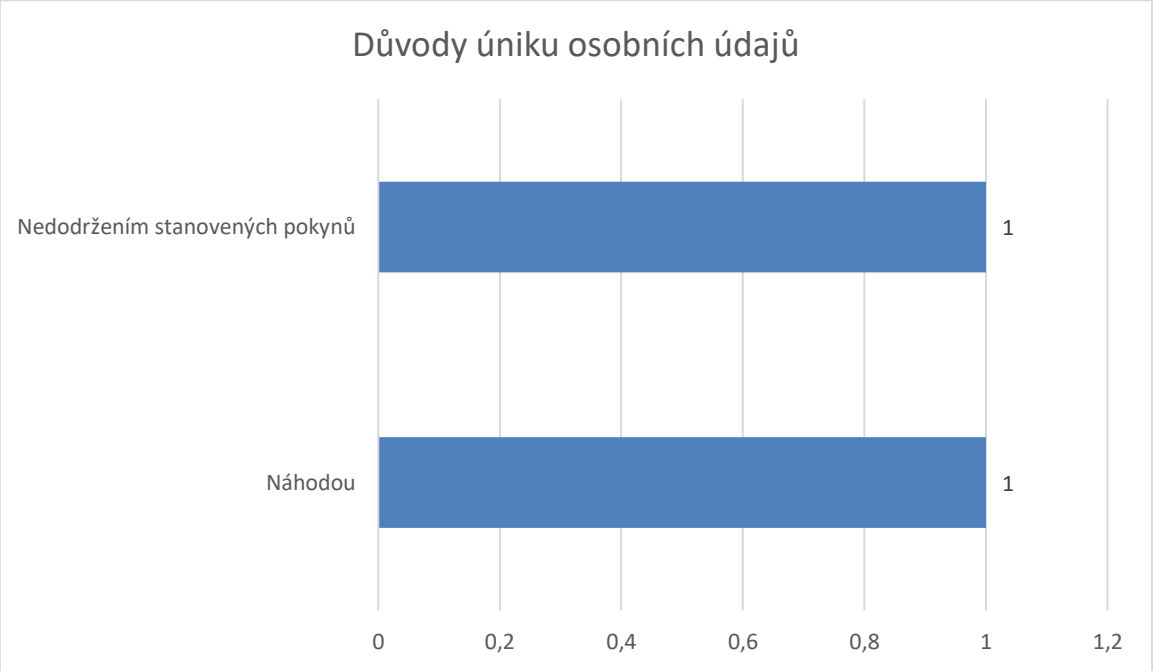
Zdroj: Vlastní zpracování

V rámci deváté otázky byly subjekty vyzvány k vyjádření, zda se v jejich škole, kdy vyskytl případ úniku osobních údajů svěřenců, jejich zástupců, zaměstnanců nebo potenciálních zájemců o studium. Jak vyplývá z výsledků, 62 subjektů uvádí, že na půdě jejich školy nikdy nedošlo k úniku osobních dat. Dva subjekty však potvrdily, že k takové situaci v minulosti došlo.

Jak je patrné, školy obvykle nejsou primárním cílem útoků hackerů, jejichž cílem je získat, pozměnit nebo vymazat osobní údaje. Nicméně mohou nastat i jiné situace, které mohou vést ke ztrátě, poškození nebo znehodnocení těchto citlivých dat, a ty nemusí být způsobeny organizovanými kybernetickými skupinami nebo osamělými hackery.

10. Otázka: Z jakého důvodu k úniku osobních údajů došlo?

Graf 10: Důvody, kvůli který došlo ke konkrétním únikům osobních údajů ze školy

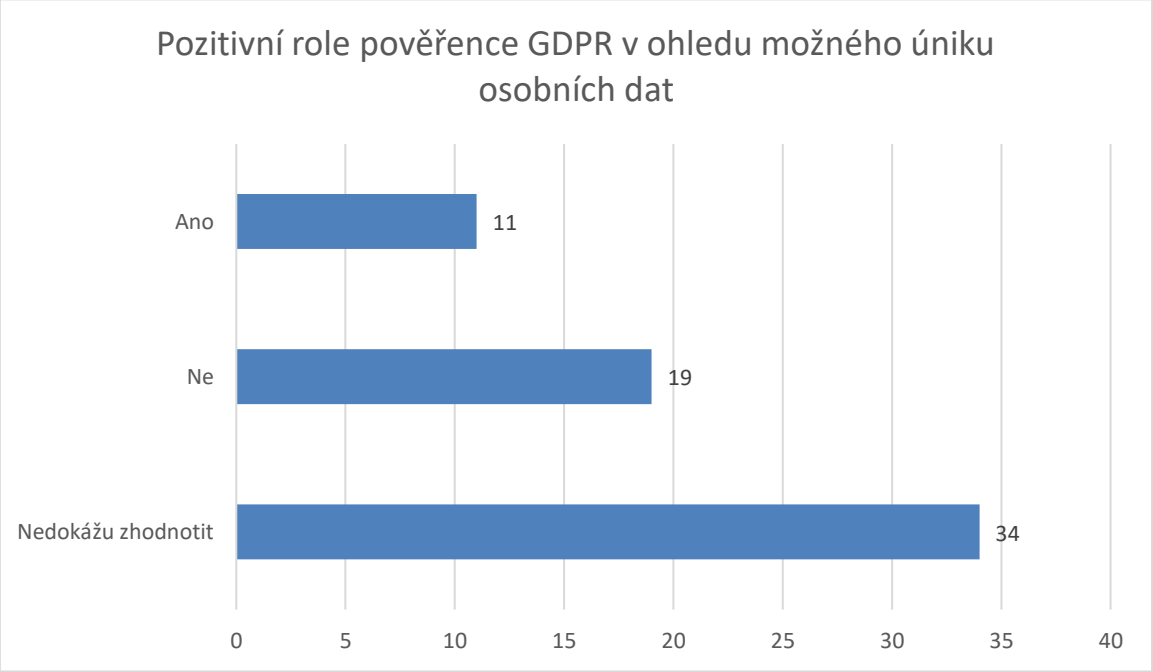


Zdroj: Vlastní zpracování

V rámci desáté otázky byly zpovídány pouze ty subjekty, které na předchozí otázku odpověděly kladně. A to, že v rámci jejich školy došlo k úniku osobních dat svěřenců. Tato otázka se ptala na konkrétní důvody, které stály za tím, že k samotnému úniku dat došlo. V rámci této otázky byla ponechána subjektům znovu volná ruka, otázka byla tzv. otevřenou, tudíž subjekty mohly samy svými slovy popsat, k jaké situaci na jejich škole došlo.
Jeden ze subjektů odpověděl, že k úniku došlo náhodou. Druhý potom, že zaměstnanec nedodržel stanovené pokyny.

11. Otázka: Jste klidnější, co se týče úniku osobních údajů poté, co byla zavedena do funkce role pověřence pro ochranu osobních údajů?

Graf 11: Pozitivní vliv pověřence GDPR v ohledu potencionálního úniku osobních dat ze školy



Zdroj: Vlastní zpracování

V rámci poslední otázce byly subjekty dotazovány na to, zda vidí zavedení role pověřence GDPR neboli odborně vyškolené a znalé osoby na ochranu osobních dat jako pozitivní, co se týče potencionálního úniku osobních dat.

11 subjektů hodnotí pozitivní dopad pověřence pro ochranu osobních údajů na snížení rizika úniku osobních údajů jako pravdivý a zároveň pociťují větší míru klidu od doby, kdy byla tato role zavedena. Devatenáct osob vyjádřilo, že od zavedení pověřence se necítí klidnější, zatímco dalších 34 osob se nerozhodlo a nemá jasný názor v této otázce.

Diskuze

V rámci výzkumné části bakalářské práce s názvem Ochrana osobních údajů ve škole byl prováděn kvantitativní průzkum pomocí dotazníkového šetření. Dotazníkové šetření mělo za úkol zjistit, jaké postupy využívá vedení současných českých škol k ochraně osobních údajů svých studentů.

Na úvod je třeba zmínit několik metodologických aspektů, které by mohly přispět k potenciálnímu zkreslení výsledků. Začněme tím, že dotazníkového průzkumu se zúčastnilo 64 respondentů. Celkový počet oslovených institucí byl 287, což naznačuje relativně vysokou návratnost dotazníků (23 %). Nicméně stále lze diskutovat o tom, zda lze 64 respondentů považovat za dostatečný počet. Je důležité si uvědomit, že se jedná o instituce, nikoli jednotlivé osoby, a proto nelze tento počet považovat za malý. Samozřejmě existuje rozdíl mezi dotazníkovým šetřením s 287 jednotlivci a 287 institucemi, a nelze považovat tyto dvě skupiny za rovnocenné.

Druhou záležitostí je, že autor vybral ucelenou skupinu, a to všechny základní školy v Ústeckém kraji, které byly zveřejněny v Rejstříku škol a školských zařízení, které spravuje Ministerstvo školství, mládeže a tělovýchovy.

Získané poznatky byly především analyzovány pomocí vizuální prezentace dat. Následně byly formulovány výzkumné otázky, které sloužily jako základ pro celkové hodnocení. Tyto otázky měly specifický charakter a zahrnovaly následující:

1. Jakým způsobem vedení školy chrání osobní údaje ve škole?

Předně je důležité zdůraznit, že z celkového počtu 287 základních škol uvedlo 46, že zajišťují zpracování a ukládání osobních údajů prostřednictvím interního pověřence pro ochranu osobních údajů, zatímco pouze 18 subjektů se spoléhá na externí pracovníky v této oblasti.

19 objektů rovněž informovalo, že pro zabezpečení a uchování osobních dat svých svěřenců využívají specializované informační systémy a software. 44 subjektů ale také upozornily, že určité osobní údaje jsou stále uchovávány v papírové formě. Pokud se tak děje, tyto papírové a fyzické dokumenty jsou uloženy na speciálně vyhrazeném místě. Přístup do místnosti s

osobními údaji, a případně k samotným dokumentům, je v rámci instituce povolen jen několika vybraným odpovědným osobám.

Pokud jde o konkrétní metody ochrany, 24 subjektů uvedlo, že mají pouze omezený počet osob s povoleným přístupem k datům. Má se na mysli úzký seznam lidí, který má přístup do povětšinou určeného archivu, kde se osobní údaje uchovávají. Stejně jako 23 má uzavřenou dohodu o mlčenlivosti. Dále 12 subjektů uvádělo, že pro ochranu osobních údajů aktivně využívají nebo jsou pověřeni orgány, které používají různé bezpečnostní technické mechanismy s cílem zabránit neoprávněnému přístupu, přenosu, ztrátě, poškození nebo jinému potenciálnímu zneužití osobních dat. Subjekty zde měly na mysli rozličné formy zabezpečení, kódování, šifrování a další bezpečnostní mechanismy, které mohou být aplikovány v informačních systémech.

2. Proč je vhodný k delegování ochrany osobních údajů pověřenec GDPR?

Subjekty jsou v názoru na zavedení funkce pověřence pro ochranu osobních údajů rozděleny přesně na polovinu.

Jako největší výhodu subjekty uvádí odbornost pověřence. Chápou ho jako jistotu v ochraně osobních údajů svěřenců. Na druhou stranu subjekty, které uváděly zavedení povinnosti pověřence jako nesprávné dále označují pověřence za zbytečnost a dle pak notnou finanční zátěž pro školy.

3. V jakých nejčastějších případech dochází k únikům osobních údajů ze škol?

Vzdělávací instituce nejsou často hlavním cílem hackerských útoků, které mají za cíl získat, pozměnit nebo vymazat data obsahující osobní údaje. Nicméně existují i jiné situace, které mohou vést k poškození, ztrátě nebo znehodnocení těchto citlivých dat, a ty nemusí být způsobeny organizovanými kybernetickými gangy nebo samostatnými hackery. Z 64 institucí uvedlo 62, že v rámci jejich škol nikdy nedošlo k úniku osobních dat nebo citlivých informací. Pouze 2 subjekty informovaly o incidentu úniku dat. V jednom případě se jednalo o náhodu a v druhém případě se jednalo o nedodržení předepsaných nařízení vztahujících se ke správě osobních údajů.

Závěr

Cílem bakalářské práce s názvem Ochrana osobních údajů ve škole bylo vytvořit komplexní a systematický přehled nejnovějších poznatků a vývoje v oblasti ochrany osobních údajů v rámci vzdělávacích institucí. Tato práce se zaměřovala na identifikaci a zhodnocení rizik spojených s ochranou osobních údajů ve školách a na návrh opatření, která by mohla předcházet nebo minimalizovat možné úniky těchto důvěrných informací.

V rámci výzkumu bylo provedeno důkladné studium literatury, analýza relevantních právních předpisů a souvisejících směrnic týkajících se ochrany osobních údajů ve školách. Následně bylo provedeno dotazníkové šetření mezi vzdělávacími institucemi, s cílem získat data ohledně jejich přístupu a opatření k ochraně osobních údajů svěřenců.

Na základě analýzy a vyhodnocení získaných informací byl vypracován návrh optimálních opatření a postupů, které by mohly být implementovány ve školách s cílem zajištění co nejefektivnější ochrany osobních údajů. Tento návrh se zaměřoval na technická opatření, jako je zabezpečení informačních systémů a datových úložišť, šifrování a kontrola přístupu k datům. Zároveň byly zohledněny i organizační a právní aspekty ochrany osobních údajů ve školách, včetně stanovení odpovědnosti, způsobu informování a školení zaměstnanců a zavedení interních kontrolních mechanismů.

Výstupy této práce slouží jako užitečný průvodce pro vzdělávací instituce při zajišťování adekvátní ochrany osobních údajů svých svěřenců a mohou být také využity při formulaci relevantních politik a postupů týkajících se ochrany dat ve školním prostředí.

V teoretické části bakalářské práce byly vysvětleny základní pojmy, které souvisejí s ochranou dat. Bylo vysvětleno, co jsou osobní údaje, co je zpracování osobních údajů i jejich ochrana. V další kapitole byl definováno a popsáno Obecné nařízení o ochraně osobních údajů (2016/679/EU) neboli Nařízení GDPR (General Data Protection Regulation). Byly vyzdviženy novinky, se kterými toto nařízení přišlo v porovnání s dříve platnou směrnicí, kterou do svého znění implementoval český zákon o ochraně dat z roku 2000, zákon č. 101/2000 Sb. a následně zákon č. 110/2019 Sb.

Novou povinností a novou osobou, která vystupuje v ochraně osobních údajů ve znění Nařízení GDPR, je tzv. pověřenec pro ochranu osobních údajů neboli Data Protection

Officer (DPO). Tato osoba má za cíl dohlížet na vzájemný soulad mezi zpracováváním osobních údajů a povinnostmi, které jsou ukotveny v rámci Nařízení GDPR.

Dále byla věnována pozornost ochraně soukromí a osobních údajů v rámci školních zařízení. Tato zařízení byla jedním z nově povinných subjektů jmenovat pověřence pro ochranu osobních údajů v souladu s Nařízením GDPR, neboť pravidelně zpracovávají rozsáhlé množství osobních údajů svých žáků, jejich zákonných zástupců a zaměstnanců. Hlavním cílem je chránit práva žáků a jejich zástupců před potenciálním neoprávněným zacházením s jejich osobními daty a poskytnout jim větší kontrolu nad tím, jak jsou jejich data využívána. Bylo identifikováno sedm hlavních principů, kterými se každá vzdělávací instituce musí řídit v souladu s Nařízením GDPR. Rovněž bylo upozorněno na možné situace, které by mohly vést k potenciálnímu úniku osobních údajů.

V rámci dotazníkového šetření, které bylo realizováno v praktické části bakalářské práce, bylo zodpovídáno 287 vzdělávacích institucí. Pozornost byla zaměřena na to, jak konkrétně školy chrání osobní údaje svých svěřenců, jaká je podle nich role pověřenců GDPR, a zda u nich došlo někdy k úniku osobních údajů.

Ze získaných poznatků lze ustanovit několik konkrétních zásad, které navýší potencionální bezpečnost osobních dat žáků:

- Osobní údaje je vhodné zpracovávat a uchovávat spíše v elektronické podobě v rámci informačních systémů.
- Papírová forma se stává častěji terčem nehod a pochybení ze strany lidského faktoru.
- Čím méně lidí má přístup k osobním údajům, tím lépe.
- Prvořadé je dodržovat naprostou profesionální mlčenlivost.
- Místnost, ve které dochází ke shromažďování dat nebo jejich ukládání, je dobré místnost zamykat, a hlídat ji kamerovým systémem.
- Vždy je dobré ponechat ochranu osobních dat na vzdělaných a zkušených odbornících.
- Důležitá je vždy řádná komunikace mezi správcem osobních dat, zpracovatelem a pověřencem pro ochranu osobních dat.
- V případě úniku dat je nutné neprodleně informovat příslušné orgány.

Seznam použitých informačních zdrojů

MATES, P, JANEČKOVÁ, E, BARTÍK, V., 2012. *Ochrana osobních údajů*. 1. vydání, Praha: Leges. ISBN: 978-80-87576-12-0.

MATOUŠOVÁ, M, HEJLÍK, L., 2008. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání, Praha: ASPI. ISBN: 978-80-7357-322-5.

MV ČR. 2000. *Základní pojmy v GDPR* [online]. [vid. 2022-10-11]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

MPO ČR. 2018. *Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů* [online]. [vid. 2022-08-11]. Dostupné z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/2018/4/GDPR_sesit_MV_1.pdf

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

NAVRÁTIL, J, a kolektiv., 2018. *GDPR pro praxi*. 1 vydání, Plzeň: Aleš Čeněk. ISBN: 978-80-7380-689-7.

NEZMAR, L., 2017. *GDPR praktický průvodce implementací*. 1 vydání, Praha: Grada Publishing. ISBN: 978-80-271-0920-3.

NULÍČEK, M, DONÁT, J, NONNEMANN, F, LICHNOVSKÝ, TOMÍŠEK, B. GDPR, 2018. *Obecné nařízení o ochraně osobních údajů*. Praktický komentář. 2 vydání, Praha: Wolters Kluwer ČR. ISBN: 978-80-271-0920-3.

Směrnice Evropského parlamentu a Rady s označením 2016/680, trestněprávní směrnice, pro oblast ochrany fyzických osob v souvislosti se zpracováním osobních údajů za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů.

Směrnice Evropského parlamentu a Rady s označením 2016/681, směrnice PNR (Passenger Name Record) pro oblast používání údajů ze jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnost.

SVOBODOVÁ, Z., 2020. *Základy metodologie výzkumu* (kvalitativní přístupy) [online]. [vid. 2023-06-18] Praha: Futurebooks, 2020. ISBN 978-80-7603-256-9. Dostupné z: https://cuni.futurebooks.cz/detail-knihy/zaklady-metodologie-vyzkumu-kvalitativnipristupy

ŠKORNIČKOVÁ, E. 2018. Proč potřebuje Evropa lepší ochranu osobních dat [online]. [vid. 2022-09-01]. Dostupné z: https://www.gdpr.cz/gdpr/proc/

Úřad pro ochranu osobních údajů. 2017. Tři nejdůležitější pojmy [online]. [vid. 2022-07-01]. Dostupné z: https://www.uoou.cz/3-nejdulezitejsi-pojmy/d-27293/p1=4744

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

ŽŮREK, J., 2017. *Praktický průvodce GDPR*. 1 vydání, Olomouc: Anag. ISBN: 978-80-7554-097-3.

Seznam příloh

Seznam obrázků

Seznam grafů