Matiční gymnázium, Ostrava, Dr. Šmerala 25	
Srovnávací analýza připravenosti MGO na GDPR	
Č.j.: GMAT/1641/2018	Účinnost od:
Spisový znak:	Skartační znak:
Změny:	

ZPRÁVA O STAVU OCHRANY OSOBNÍCH ÚDAJŮ VE VZTAHU K POŽADAVKŮM GDPR

MATIČNÍ GYMNÁZIUM, OSTRAVA, PŘÍSPĚVKOVÁ ORGANIZACE

Matiční gymnázium, Ostrava, příspěvková organizace
Dr. Šmerala 25, 728 04 Ostrava

Telefon: **596 116 239**
Bankovní spojení: **KB Ostrava 8036761/0100**
IČO: **00842761**
E-mail: **info@mgo.cz**
Web **www.mgo.cz**

Obsah

1. VÝSLEDKY SROVNÁVACÍ ANALÝZY PŘIPRAVENOSTI MGO NA GDPR 4
1.1 Úvod 4
1.2 Klíčová zjištění v připravenosti MGO na GDPR 4
1.3 Identifikace zpracování 5
1.4 Zjištění navrhovaných právních základů 5
1.5 Posouzení stavu dokumentace 5
1.6 Stav informací zveřejněných na webových stránkách 7
1.7 Posouzení stavu stávajících interních systémů 7
1.8 Mapování osobních údajů v systémech 7
1.9 Stav podávaných informací 7
1.10 Stav zpracovatelských smluv 8
1.11 Stávající podmínky pro řízení bezpečnostních incidentů 8
1.12 Stav agendy DPO 8
1.13 Stav stávajících opatření ke zpracování a ochraně osobních údajů 8
2. ZÁKLADNÍ USTANOVENÍ 9
2.1 Umístění a ochrana dokumentu 9
2.2 Verze dokumentu 9
2.3 Účel analýzy 9
2.4 Seznam rolí 10
2.5 Hodnocení stavu ochrany osobních údajů 10
2.6 Aktuální stav v registru zpracování osobních údajů 10
2.7 Srovnávací analýza 11
2.8 Dopadová analýza 11
3. GAP ANALÝZA 13
3.1 Cíl provedení analýzy 13
3.2 Způsob posouzení 13
3.3 Vstupní informace 13
3.4 Kontroly dozorovým úřadem v souvislosti s GDPR 14
4. VÝSLEDKY GAP ANALÝZY 16
4.1 Základní přehled identifikovaných zpracování 16
4.2 Identifikovaná zpracování 16
4.2.1 Správní řízení 16
4.2.2 Maturitní zkoušky 19
4.2.3 Školní matrika a vzdělávání 22
4.2.4 Agenda výchovného poradce a školního metodika prevence 25
4.2.5 Školní akce a zájezdy 28
4.2.6 Projektová činnost 30
4.2.7 Pojistné události a úrazy 33
4.2.8 Personální a platová agenda 36
4.2.9 Inventarizace 39
4.2.10 Příprava a uzavírání smluvních vztahů 42
4.3 Informační povinnost 45
4.3.1 Plnění informační povinnosti správce podle GDPR 45
4.3.2 Možné řešení informační povinnosti podle GDPR 45
4.3.3 Doporučujeme další informace dle čl. 13 GDPR, zejména: 46
4.4 Stav zpracovatelských smluv 47

4.5 Přijatá technická a organizační opatření 48
4.6 Personální bezpečnost 48
4.7 Fyzická bezpečnost 49
4.8 Administrativní bezpečnost 49
4.9 Bezpečnost IT aplikací a systémů 50
4.10 Opatření pro likvidaci osobních údajů 50
4.11 Doporučení pro plnění povinností správce při zabezpečení zpracování osobních údajů v rozsahu požadavků čl. 32 GDPR 51
4.12 Kontrolní činnost 52
5. NÁVRHY ŘEŠENÍ 54
5.2 Pověřenec pro ochranu osobních údajů 54
5.3 Postavení pověřence pro ochranu osobních údajů 54
5.4 Doporučení personálního obsazení 55
5.5 Vlastní zaměstnanec 55
5.6 Externista na základě smlouvy o poskytování služeb 55
5.6.1 Vlastní zaměstnanec s externí podporou 55
5.7 Návrh katalogu činností pověřence pro ochranu osobních údajů 56
5.8 Záznamy o činnostech zpracování 57
5.9 Záznamy o činnostech vedené správcem 58
5.10 Záznamy o činnostech vedené zpracovatelem 58
5.11 Návrh procesů k hlášení narušení bezpečnosti osobních údajů 59
5.11.1 Řešení bezpečnostního incidentu 60
5.12 Návrh rozhodovacího procesu při uplatňování práv subjektů údajů 60
5.12.1 Právo být informován o zpracování osobních údajů 60
5.12.2 Právo na přístup k osobním údajům 61
5.12.3 Právo na opravu nepřesných osobních údajů 62
5.12.4 Právo na výmaz (být zapomenut) 62
5.12.5 Právo na omezení zpracování 63
5.12.6 Právo na přenositelnost 63
5.12.7 Právo vznést námitku 64
5.12.8 Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování 65
5.12.9 Společná ustanovení k rozhodovacím procesům 65
5.13 Návrh rozhodovacího procesu pro realizaci posouzení vlivu na ochranu osobních údajů 66
5.13.1 Návrh rozhodovacího procesu 66
5.13.2 Metodika pro případné posouzení vlivu na ochranu osobních údajů 67
5.14 Návrh metodiky a postupu pro realizaci záměrné ochrany 69
5.14.1 Vznik nových zpracovatelských operací nebo změna již existujících 69
5.14.2 Zánik zpracovatelské operace nebo jakékoli její části 69
5.15 Návrh metodiky a postupu pro realizaci standardní ochrany 70
5.15.1 Základní pravidla fyzické bezpečnosti 70
5.15.2 Základní pravidla personální bezpečnosti 70
5.15.3 Základní pravidla administrativní bezpečnosti 71
5.15.4 Základní pravidla bezpečnosti IT 71
5.16 Návrh procesů k zajištění pravidelného testování a vyhodnocování účinnosti přijatých technických a organizačních opatření 71
6. ANALÝZA A ŘÍZENÍ RIZIK 72
6.1 Analýza rizik – metodická východiska 72
6.2 Klasifikace rizik a jejich dopadů 73
6.3 Hodnocení rizik 74

6.4 Eliminace rizik **78**

7. ZÁVĚR A DOPORUČENÍ K DALŠÍMU POSTUPU **81**

7.1 Nutné kroky dalšího postupu **81**

7.2 Informace zveřejněné na webových stránkách MGO **82**

7.3 Posouzení stavu stávajících interních systémů **82**

7.4 Stávající podmínky pro řízení bezpečnostních incidentů **83**

8. PŘÍLOHA – DOPORUČENÍ KE KAMEROVÉMU SYSTÉMU **84**

9. POUŽITÉ TERMÍNY, ZKRATKY A POJMY **86**

1. VÝSLEDKY SROVNÁVACÍ ANALÝZY PŘIPRAVENOSTI MGO NA GDPR

1.1 ÚVOD

Listina základních práv Evropské unie a Smlouva o fungování Evropské unie (EU) přiznávají každému právo na ochranu osobních údajů (dále též „OÚ"), které se jej týkají. K zajištění tohoto práva bylo přijato NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, v anglickém jazyce General Data Protection Regulation – GDPR).

Ačkoliv cíle a zásady směrnice 95/46/ES, z níž vychází i zákon České republiky č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále též „ZOOÚ"), nadále platí, nezabránilo to roztříštěnosti v provádění ochrany údajů v celé EU, právní nejistotě ani rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud jde o činnosti prováděné online prostřednictvím informačních technologií. Práva jednotlivců k ochraně jejich osobních údajů jsou novým nařízením výrazně posílena.

Cílem srovnávací analýzy s požadavky GDPR (dále jen „srovnávací analýza") bylo provést strukturované srovnání existujícího stavu ochrany osobních údajů na Matičním gymnáziu, Ostrava, příspěvková organizace, Dr. Šmerala 25, 728 04 Ostrava **(dále jen MGO)** se stavem požadovaným nařízením GDPR. Byl posouzen stávající stav plnění požadavků na zpracování osobních údajů na MGO a touto analýzou byla stanovena metodika dalšího postupu pro ochranu osobních údajů fyzických osob v souvislosti s jejich zpracováním a ochranou.

Při provádění srovnávací analýzy jsme vycházeli výhradně z informací, které máme dle současné legislativy k dispozici a v kompetenci řešení.

Analyzované smlouvy lze obecně charakterizovat jako smlouvy mezi dodavatelem a odběratelem popisující charakter dohody bez ustanovení, požadovaných nařízením GDPPR z hlediska zpracování osobních údajů na konkrétní období. Na základě analýzy budeme uzavírat dodatky ke smlouvám řešící požadavky GDPR – zejména upřesnit udělení souhlasu se zpracováním osobních údajů na období se specifikovaným termínem ukončení udělení souhlasu.

1.2 KLÍČOVÁ ZJIŠTĚNÍ V PŘIPRAVENOSTI MGO NA GDPR

V rámci analýzy připravenosti na GDPR byla provedena GAP analýza souladu s tímto nařízením. Byl posouzen stávající stav zpracování osobních údajů a stávající míra plnění požadavků GDPR. MGO musí:

- vytvořit katalog (záznamy) zpracování;
- vést interní záznamy o činnostech zpracování;
- jmenovat pověřence pro ochranu osobních údajů;
- uzavřít zpracovatelské smlouvy;
- doplnit na www stránkách právní ochranu osobních údajů;

- upravit proces udělování souhlasu na www stránkách se zpracováním osobních údajů;
- upravit politiku sledování uživatelů na webu – cookies;
- zavést procesy stanovené GDPR v rámci organizace jako:
    - právo na přístup;
    - právo na výmaz;
    - právo námitky;
    - právo pozastavení;
    - právo na informace;
    - právo přenositelnosti.
- přijmout technická a organizační opatření snižující rizika pro subjekty údajů;
- proškolit zaměstnance SŠ z hlediska ochrany osobních údajů;
- upravit retenční doby (doba uchování) údajů a zavést do spisového řádu;
- vypracovat analýzu rizik zpracování;
- kde je třeba, vytvořit Balanční testy;
- kde je třeba, vytvořit Posouzení vlivu pro ochranu osobních údajů;
- zavést proces ohlášení porušení zabezpečení osobních údajů;
- zavést systém řízení incidentů z pohledu GDPR.

1.3 IDENTIFIKACE ZPRACOVÁNÍ

Celkově bylo identifikováno 11 procesů zpracování v rámci MGO, které byly kategorizovány do 11 scénářů zpracování.

1.4 ZJIŠTĚNÍ NAVRHOVANÝCH PRÁVNÍCH ZÁKLADŮ

Na MGO lze ze šesti možných právních základů zpracování běžných osobních údajů využít čtyři. Udělení souhlasu subjektem údajů, zpracování založené na právním základu veřejného zájmu správce, zpracování postavené na právních povinnostech správce a zpracování vycházející z plnění smlouvy.

1.5 POSOUZENÍ STAVU DOKUMENTACE

MGO provedla analýzu následující dokumentace vztahující se k ochraně osobních údajů:

- Organizační řád včetně příloh
- Smlouva Bakaláři včetně příloh a dodatků

- Formulář DPP
- Formulář pracovní smlouvy
- Mzdový list
- Osobní dotazník žáka, zaměstnance (vstupní)
- Formulář Souhlas se zpracováním osobních údajů pro potřeby MGO
- Směrnice o ochraně osobních údajů
- Smlouva Vema a. s.
- Smlouva Elanor s. r. o.
- Smlouva T-mobile
- Registrace na web4you.cz
- Souhlas rodičů nezletilých žáků s činností výchovného poradce
- Souhlas rodičů nezletilých žáků se sociometrickými analýzami vztahů uvnitř třídních kolektivů
- Souhlas rodičů nezletilých žáků s působením školního psychologa
- Souhlas s opuštěním budovy
- Vyjádření žáka/zákonného zástupce – souhlas se zpracováním OÚ

Doporučený rozsah dokumentace vhodné z hlediska nařízení GDPR, průběžně aktualizované a dostupné pro případ kontroly ze strany ÚOOÚ by měl obsahovat:

- GAP Analýzu souladu s GDPR;
- Popis identifikovaných zpracování;
- Katalog těchto zpracování;
- Analýzu rizik scénářů zpracování z hlediska subjektů údajů;
- Popis přijatých opatření;
- Důkazy prokazující aktivní přístup k řešení ochrany osobních údajů jako například potvrzení prokazující proškolení zaměstnanců SŠ v této oblasti;
- Doplňující dokumenty, pokud jsou třeba, jako
    - Balanční testy u zpracování založených na oprávněných zájmech; nebo
    - Posouzení vlivu na ochranu osobních údajů u zpracování vyhodnocených jako kritické;
- Popisy procesů vedoucích k naplnění práv subjektů údajů;
- Vzorové dokumenty:
    - Zpracovatelské smlouvy;

- Udělované souhlasy;
- Dohodu o mlčenlivosti.

1.6 STAV INFORMACÍ ZVEŘEJNĚNÝCH NA WEBOVÝCH STRÁNKÁCH

Současné webové stránky z hlediska GDPR nesplňují požadavky na internetové řešení kladené. Vytvoření dokumentace pro webovou sekci „Ochrana OÚ" bude zpracována a dodána centrálně zřizovatelem (do 11. 5. 2018. Dále budou ověřeny souhlasy udělené zaměstnanci i klienty pro zveřejnění fotografií na internetových stránkách.

1.7 POSOUZENÍ STAVU STÁVAJÍCÍCH INTERNÍCH SYSTÉMŮ

Současná infrastruktura a systémy na MGO obecně splňují většinu požadavků GDPR na bezpečnost zpracování osobních údajů. Nově budou doplněny primárně procesní věci, tzn. definován systém řízení kontinuity činností, vytvořena odpovídající sada dokumentů a zapracována případná opatření vyplývající z nalezených rizik zpracování.

1.8 MAPOVÁNÍ OSOBNÍCH ÚDAJŮ V SYSTÉMECH

V procesu pro řízení a uspokojení práv subjektů na výmaz, pozastavení či přenos budeme nuceni učinit dílčí úpravy v architektuře informačních systémů organizace. Jde o větší či menší zásahy, které je nutné udělat, aby došlo k centralizaci zpracování osobních údajů v rámci systémů. Bude tak výrazně jednodušší řešit případné změny na základě vyžadovaných práv pro výmaz, pozastavení zpracování či přenos údajů.

Poskytovatelům aplikací a informačních systémů byl položen závazný dotaz na připravenost jimi dodaných či spravovaných informačních systémů a aplikací pro MGO. Zpracovatelské firmy potvrdily připravenost IS – deklarace dodavatelů

Dodavatel	Aplikace / IS	Deklarace připravenosti
Elanor spol. s r.o.	IS FAUST (účetní s.)	bude připraveno do účinnosti nařízení GDPR
ICZ a.s.	Spisová služba e-spis LITE	bude připraveno do účinnosti nařízení GDPR
Vema, a.s.	personální a mzdový IS Vema	bude připraveno do účinnosti nařízení GDPR
TESCO SW a.s.	IS FaMa+	bude připraveno do účinnosti nařízení GDPR
BAKALÁŘI software, s. r. o	Bakaláři	bude připraveno do účinnosti nařízení GDPR

1.9 STAV PODÁVANÝCH INFORMACÍ

MGO v současné době v absolutní většině případů plní povinnost informovanosti vůči subjektům údajů v souladu se zákonem o ochraně osobních údajů. Správce je povinen informace poskytnout nejpozději

momentem prvního kontaktu nebo do jednoho měsíce a informace poskytnout subjektu údajů, když jsou vyžádány.

1.10 STAV ZPRACOVATELSKÝCH SMLUV

Zpracovatelské smlouvy a dodatky obsahují z hlediska potřeb stanovených nařízením GDPR pouze velmi obecná ustanovení. MGO provede revize smluv a případně uzavře se zpracovateli dodatečné zpracovatelské smlouvy obsahující ustanovení o povinnosti zpracovatele stanovené nařízením GDPR v dostatečném rozsahu. Provedení změn ve vzorových dodavatelských smlouvách bude zřizovatelem provedeno centrálně. Bude se jednat o doplnění nových položek ohledně zpracování osobních údajů a mlčenlivosti ohledně osobních údajů. Vzorové doložky budou centrálně dodány zřizovatelem.

1.11 STÁVAJÍCÍ PODMÍNKY PRO ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Proces řízení bezpečnostních incidentů z hlediska GDPR není na MGO definován. V současné době nejsou všechny aplikace a informační systémy technicky připravené na pokrytí veškerých požadavků, které na tento proces nařízení GDPR klade.

1.12 STAV AGENDY DPO

V současné době nemá MGO jmenovaného pověřence pro ochranu osobních údajů. Vzhledem k povinnosti státní správy a podřízených organizací jej jmenovat, jsme připraveni tuto povinnost splnit. Jmenování pověřence umožní snazší komunikaci s orgány dohledu i subjekty údajů.

Jmenování pověřence pro ochranu osobních údajů zajistí v počátcích účinnosti GDPR zřizovatel (18. 5. 2018).

1.13 STAV STÁVAJÍCÍCH OPATŘENÍ KE ZPRACOVÁNÍ A OCHRANĚ OSOBNÍCH ÚDAJŮ

Na základě námi provedené srovnávací analýzy realizujeme další kroky v oblasti ochrany osobních údajů, které budou eliminovat zjištěné neshody s GDPR. Návrh dalších kroků a metodiky uvádíme v kapitole č. 7.

2. ZÁKLADNÍ USTANOVENÍ

2.1 UMÍSTĚNÍ A OCHRANA DOKUMENTU

Dokument, který obsahuje neveřejné informace musí být uchováván, přenášen a distribuován v souladu s pravidly pro ochranu informací, platnými v podmínkách SŠ.

Tyto informace nesmí být bez předchozího svolení MGO postoupeny třetí straně. Nesmí být používány či rozmnožovány pro jiné účely než za účelem posouzení dokumentu.

2.2 VERZE DOKUMENTU

Tabulka číslo 1 **Verze dokumentu**

Autor	Datum	Verze	Popis změny
	20. 2. 2018	1.0	Tvorba dokumentu

2.3 ÚČEL ANALÝZY

Účelem analýzy je na základě zjištěného stavu na MGO zhodnotit stávající kvalitu procesů a opatření z hlediska požadavků GDPR a posoudit plnění požadavků GDPR.

Naše analýzy dále obsahuje metodiky hodnocení plnění požadavků GDPR, popis způsobu zpracování zprávy srovnávací analýzy a návrhy spolu s doporučeními, aby systém administrace MGO plně odpovídal požadavkům GDPR.

Zjištěná skutková podstata bude sloužit jako podklad pro plnění povinností vyplývajících z Obecného nařízení o ochraně osobních údajů – GDPR. Provedená analýza stavu ochrany osobních údajů na MGO napovídá, že je nutno realizovat následující:

- přijmout plán implementace požadavků GDPR, včetně stanoveného harmonogramu a nezbytné alokace zdrojů;
- ustanovit po dobu implementace požadavků GDPR funkci (roli) projektového manažera GDPR;
- jmenovat pověřence pro ochranu osobních údajů;
- doplnit identifikace jednotlivých zpracování osobních údajů, pokud dojde k dodatečnému zjištění;
- na základě identifikace jednotlivých zpracování určit odpovědné osoby za tato zpracování;
- provést hodnocení rizik zpracování na základě dokončené identifikace;

- na základě výsledku hodnocení rizik vyhodnotit, zda je u zpracování s vysokým rizikem nezbytné přistoupit k vypracování případného Posouzení vlivu na ochranu osobních údajů;
- realizovat doporučené změny v dokumentaci, směrnicích a smlouvách;
- přijmout případná doporučená opatření směřující k zabezpečení ochrany osobních údajů;
- proškolit zaměstnance MGO v oblasti ochrany osobních údajů;
- akceptovat pravidelný interní audit či jinou kontrolu nakládání s osobními údaji;
- postupovat při implementaci dle navrhovaných metodik.

2.4 SEZNAM ROLÍ

Tabulka číslo 2 **Seznam rolí**

Role	Popis
Správce	Právně odpovědný za celkovou implementaci požadavků spojených s GDPR včetně formální validace – SŠ
Manažer GDPR	Odpovídá za implementační plán, průběh implementace požadavků GDPR, navrhuje procesy, postupy a metodiky, odpovídá za hodnocení rizik
Pověřenec pro ochranu osobních údajů (DPO)	Schvaluje navržené postupy a procesy, dává posudky k navrhovaným opatřením a postupům, komunikuje se subjekty údajů a dohledovým orgánem, nastavuje lhůty, povoluje a schvaluje konkrétní postupy
Manažer kybernetické bezpečnosti	Konzultační a informační role, spolupodílí se na identifikaci zdrojů rizik a hrozeb v oblasti IT

2.5 HODNOCENÍ STAVU OCHRANY OSOBNÍCH ÚDAJŮ

Základním cílem hodnocení stavu ochrany osobních údajů je zajistit do budoucna její potřebnou úroveň a zajistit prosazování ochrany osobních údajů na MGO. Přitom zajištěním ochrany osobních údajů se rozumí soustavné snižování rizik (ztráty, poškození a zneužití údajů, poškození práv subjektů údajů atd.) spojených se zpracováním osobních údajů v informačních systémech (dále též „IS") a dále obsažených v listinných dokumentech.

Hodnocení stavu ochrany OÚ je charakterizováno jako soustava organizačních a technických opatření, která zajišťují shromáždění a vyhodnocení informací o stavu ochrany OÚ dle předem stanoveného rozsahu a pravidla pro jejich posuzování a hodnocení.

2.6 AKTUÁLNÍ STAV V REGISTRU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

MGO není registrována v registru zpracování osobních údajů vedeném ÚOOÚ.

2.7 SROVNÁVACÍ ANALÝZA

V této srovnávací analýze posuzujeme úroveň stavu ochrany OÚ dle stanoveného rozsahu GDPR. Skutečnosti zjištěné při srovnávací analýze nám poskytnou informace o slabinách a nedostatcích v zajištění ochrany OÚ MGO. Kritéria srovnávací analýzy vychází zejména z GDPR a souvisejících legislativních požadavků.

2.8 DOPADOVÁ ANALÝZA

V této kapitole uvádíme speciální ustanovení GDPR, která se uplatňují při zpracování osobních údajů na Matičním gymnáziu, Ostrava.

Omezené využití právního titulu oprávněných zájmů

Jedním z právních titulů pro zpracování osobních údajů jsou oprávněné zájmy příslušného správce či třetí strany. Tyto zájmy však nesmí převážit nad zájmy nebo základními právy a svobodami subjektu údajů. Toto obecné omezení, které je adresováno všem správcům osobních údajů GDPR doplňuje ještě zákazem orgánům veřejné moci využít zmíněný právní titul pro zpracování osobních údajů při plnění jejich úkolů. Orgány veřejné moci však smí uvedený právní titul využít v případě, kdy vystupují jako účastník soukromoprávních vztahů.

Omezení práva být zapomenut

Právo být zapomenut uplatňují subjekty údajů v rámci mantinelů stanovených GDPR. Nejde tedy o právo absolutní a jeho výkon se odvíjí od dalších skutečností. V případě specifik zpracování osobních údajů krajem může být právo být zapomenut omezeno také z důvodu splnění právní povinnosti, která se na správce vztahuje, nebo pro splnění kolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen, pokud je zpracování osobních údajů v takových případech nezbytné. Právo být zapomenut je omezeno také v souvislosti s povinností organizace uchovávat dokumenty a umožnit výběr archiválií podle zákona o archivnictví a spisové službě.

Omezení práva na přenositelnost údajů

Toto právo nelze realizovat u aktivit nezbytných pro splnění povinností či úkolu upravených zákonem.

Povinnost jmenovat pověřence pro ochranu osobních údajů

Povinnost jmenovat pověřence pro ochranu osobních údajů platí pro všechny orgány veřejné moci a veřejné subjekty bez ohledu na to, jaké osobní údaje a v jakém rozsahu zpracovávají. Pověřenec zejména monitoruje soulad zpracování osobních údajů s GDPR a dalšími souvisejícími právními předpisy a poskytuje poradenství v souvislosti se zpracováním osobních údajů správci nebo zpracovateli a jejich zaměstnancům.

Plnění informační povinnosti zveřejněním

Plnění informační povinnosti tímto způsobem bude možné pouze tehdy, pokud budou zpracovávány osobní údaje v rámci úkolů stanovených kraji právními předpisy nebo při výkonu veřejné moci.

Snížení sankcí

Zákona o zpracování osobních údajů také pro orgány veřejné moci a veřejné subjekty snižuje horní hranici pokut, které lze uložit za porušení povinností stanovených GDPR, a to na 10 mil. Kč. Uplatnění správních sankcí nevylučuje uplatnění nároku v civilním řízení.

3. GAP ANALÝZA

3.1 CÍL PROVEDENÍ ANALÝZY

Cílem provedení analýzy současného stavu zpracování a ochrany osobních údajů na MGO je vytvořit výchozí podmínky pro implementaci 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) – General Data Protection Regulation (dále jen „GDPR") při ochraně osobních údajů na Matičním gymnáziu, Ostrava.

3.2 ZPŮSOB POSOUZENÍ

V rámci srovnávací analýzy byl posuzován jednak stav plnění právních povinností souvisejících se zpracováním osobních údajů a zároveň stav zavedení organizačních (procesních) a technických ochranných opatření vyžadovaných GDPR.

Procesy a opatření GDPR byly posuzovány na základě porovnání současného stavu s legislativními požadavky, a to dle požadavků stanovených vedením MGO, kterými jsou:

- Identifikace zpracování;
- Zjištění navrhovaných právních základů;
- Posouzení současného stavu dokumentace;
- Zjištění probíhajících klíčových iniciativ a základní návrh jejich zařazení do českého prostředí;
- Stav informací zveřejněných na webových stránkách MGO;
- Posouzení stavu stávajících interních systémů;
- Mapování osobních údajů v systémech;
- Stav podávaných informací;
- Stav zpracovatelských smluv;
- Stávající podmínky pro řízení bezpečnostních incidentů;
- Stav agendy pověřence (DPO);
- Stav stávajících opatření ke zpracování a ochraně osobních údajů.

V závěru GAP analýzy je popsán návrh dalšího postupu.

3.3 VSTUPNÍ INFORMACE

Pro provedení srovnávací analýzy byly informace o procesech a opatřeních získávány detailní kontrolou současného stavu v kontextu kompatibility s obsahovým rámcem GPDR.

Pohled přes požadavky GDPR: plnění jednotlivých požadavků GDPR a hodnocení stávajících opatření pro ochranu osobních údajů – bezpečnostní politika, organizace bezpečnosti, bezpečnost lidských zdrojů, fyzická bezpečnost a bezpečnost prostředí, kryptografie, řízení komunikací, řízení provozu, řízení přístupu, akvizice, vývoj a údržba informačních systémů, dodavatelské vztahy, zvládání bezpečnostních incidentů, řízení kontinuity činností organizace a řízení souladu s požadavky;

- **Pohled přes služby a interní systémy byl proveden na základě organizační a řídící struktury MGO –** tento systém jasně vymezuje pozice a povinnosti jednotlivých organizačních článků ve vztahu ke GDPR.

Zjištění stavu bylo převážně provedeno následujícími technikami:

- ze studia dostupných relevantních podkladových materiálů a metodických doporučení MŠMT ČR,
- z vedení strukturovaných rozhovorů s vybranými pracovníky na jednotlivých pozicích,
- z posuzování a rozboru získávaných informací,
- ze zpracování získaných informací do strukturované podoby.

Tabulka číslo 3 **Přehled respondentů pro identifikaci jednotlivých zpracování**

Jméno	**pozice**
	Ředitelka školy

3.4 KONTROLY DOZOROVÝM ÚŘADEM V SOUVISLOSTI S GDPR

Povinností každého členského státu Evropské unie je zřídit dozorový úřad. V současné době je v ČR takovým úřadem Úřad pro ochranu osobních údajů a jeho povinnosti a kompetence jsou zakotveny ve stávajícím zákoně o ochraně osobních údajů.

Obdobné skutečnosti jsou zakotveny i v kap. VI GDPR Nezávislé dozorové úřady. Podle čl. 57 GDPR každý dozorový úřad na svém území mj.:

- monitoruje a vymáhá uplatňování GDPR,
- zabývá se podanými stížnostmi,
- prošetřuje předmět stížnosti,
- provádí šetření o uplatňování GDPR, mj. na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci.

Z výše uvedeného lze dovodit, že dozorový orgán bude své kompetence při vymáhání uplatňování GDPR provádět obdobným způsobem, jako stávající Úřad pro ochranu osobních údajů, tj.:

- na základě plánu kontrolní činnosti, a

- na základě podání podnětu.

Zda bude MGO zahrnuto do plánu kontrolní činnosti dozorového úřadu na rok 2018 či dále nelze predikovat, stejně tak nelze vyloučit kontrolu dozorovým úřadem na základě podnětu podaného například nespokojeným klientem nebo zaměstnancem.

- Upřesnění výše uvedeného je předmětem adaptačního zákona, který má nahradit stávající zákon o ochraně osobních údajů.

4. VÝSLEDKY GAP ANALÝZY

Tato kapitola obsahuje výsledky srovnávací analýzy. Obsahuje zjištění identifikovaná porovnáním současného stavu ochrany osobních údajů a požadavků GDPR v rámci činnosti Matičního gymnázia, Ostrava, příspěvková organizace, Dr. Šmerala 25, Ostrava 7028 04.

4.1 ZÁKLADNÍ PŘEHLED IDENTIFIKOVANÝCH ZPRACOVÁNÍ

V rámci interní komplexní analýzy souladu požadavků GDPR s aktuálním systémem nakládání s OÚ na MGO, byly identifikovány tyto zákony a vyhláškami vymezené administrativní operace zpracování osobních údajů. Ty jsme pro přehlednost rozdělily do tzv. Základního přehledu identifikovaných zpracování:

Obrázek číslo 1 **Základní přehled identifikovaných zpracování**

p. č.	označení	identifikované zpracování
1	4.2.1	Správní řízení
2	4.2.2	Maturitní zkoušky
3	4.2.3	Školní matrika a vzdělávání
4	4.2.4	Agenda výchovného poradce a školního metodika prevence
5	4.2.5	Školní akce a zájezdy
6	4.2.6	Projektová činnost
7	4.2.7	Pojistné události a úrazy
8	4.2.8	Personální a platová agenda
9	4.2.9	Inventarizace
10	4.2.10	Příprava a uzavírání smluvních vztahů

4.2 IDENTIFIKOVANÁ ZPRACOVÁNÍ

4.2.1 SPRÁVNÍ ŘÍZENÍ

Rozhodnutí ředitele školy (přijímací řízení, přestupy žáků, přerušení studia, opakování ročníku), evidence a zpracování žádostí a spisů, komunikace s účastníky řízení a jejich zástupci, dotčenými osobami a orgány, doručování dokumentů, vedení řízení ústních jednání, realizace procesních úkonů, vydání správních rozhodnutí, založení spisů.

4.2.1.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. Žádný další subjekt nebyl identifkován v pozici zpracovatele.

4.2.1.2 ÚČEL ZPRACOVÁNÍ

Evidence a vydávání rozhodnutí na základě plnění právní povinnosti.

4.2.1.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:

- klienti / zákazníci
- Jiné osoby: zmocněnci, rodinní příslušníci, zájemci o vzdělání, žadatelé / stěžovatelé

- kategorie osobních údajů:
  - jméno
  - příjmení
  - titul
  - rodné číslo
  - datum narození
  - místo narození
  - vzdělání
  - email
  - telefon
  - adresa
  - podpis

4.2.1.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracovávaných údajů se pohybuje v řádu cca 500 ročně a nejedná se o systematické zpracování. Rozsah osobních údajů je přiměřený k účelu jejich zpracování.

4.2.1.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů:

- Rasový / etnický původ
- Zdravotní stav

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.1.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě – jako pomocná evidence
- Pomocných kancelářských aplikacích: word, excel
- Informačním systému v aplikacích: BAKALÁŘI, E-spis LITE ICZ, CZVV.

4.2.1.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování 5 – 10 let podle dílčího scénáře v souladu se spisovým a skartačním řádem.

Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.1.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že osobní data jsou sdílena s ostatními pracovníky školy, a to v souladu s organizačním řádem MGO.

4.2.1.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené analýzy aktuálního stavu jsou případné incidenty řešeny a je stanoven proces korekce případného porušení zabezpečení údajů.

4.2.1.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

MSK (zřizovatel MGO) má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.1.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti ze strany správce.

Právo na výmaz je implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že MSK již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.1.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání
- Validace, kontrola
- Používání
- Předávání
- Nahlížení

4.2.1.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

Pro zajištění všech administrativních operací jsou vybrané údaje poskytovány třetím osobám na základě právní povinnosti.

4.2.1.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou předávány do třetích zemí.

4.2.1.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.1.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	2	1	1	nízké
ztráta údajů	2	1	1	nízké
pozměňování údajů	1	1	1	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	1	nízké
neoprávněné zpřístupnění uložených údajů	1	1	1	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	1	nízké
neoprávněný přístup k údajům	1	1	1	nízké

4.2.2 MATURITNÍ ZKOUŠKY

Údaje z přihlášek k maturitě předávané CVVZ, zpracování maturitní dokumentace - seznamy žáků, rozpisy, protokoly, komunikace, výkon zkoušky, seznámení s výsledkem, zpracování žádostí o přezkoumání, součinnost s nadřízenými orgány.

4.2.2.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele byl identifikován externí subjekt – CVVZ.

4.2.2.2 ÚČEL ZPRACOVÁNÍ

Evidence a administrativa maturitních zkoušek, archivace výsledků MZ.

4.2.2.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - klienti / zákazníci
  - jiné osoby: zmocněnci, žadatelé, stěžovatelé
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - datum narození
  - místo narození

- rodné číslo
- vzdělání
- email
- telefon
- adresa
- podpis

4.2.2.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca 150 ročně. Jedná se o zpracování systematické.

4.2.2.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů – zdravotní stav. Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.2.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikacích E-spis LITE ICZ, BAKALÁŘI, CZVV - aplikace pro maturitní zkoušky.

4.2.2.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena na 45 let v souladu se Spisovým a skartačním řádem. Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.2.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny s ostatními pracovníky školy.

4.2.2.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.2.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.2.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.2.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání
- Validace
- Používání
- Předávání
- Nahlížení

4.2.2.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje jsou poskytovány třetím osobám - CVVZ.

4.2.2.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.2.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.2.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.3 ŠKOLNÍ MATRIKA A VZDĚLÁVÁNÍ

Školní matrika, evidence údajů o žácích, zpracování katalogů, studijních výkazů a třídních knih, agenda třídních učitelů.

4.2.3.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele byly identifikovány externí subjekty:

- BAKALÁŘI
- MSK v roli zřizovatele

4.2.3.2 ÚČEL ZPRACOVÁNÍ

Evidence a administrativa údajů o vzdělávání.

4.2.3.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - zaměstnanci
  - klienti / zákazníci
  - jiné osoby: zmocněnci, rodinní příslušníci, žadatelé, stěžovatelé
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - datum narození
  - místo narození
  - rodné číslo
  - vzdělání
  - email
  - telefon
  - adresa
  - podpis

4.2.3.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca stovky měsíčně. Jedná se o zpracování systematické.

4.2.3.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů¨:

- Rasový / etnický původ
- Zdravotní stav

Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.3.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikacích E-spis LITE ICZ, BAKALÁŘI, CZVV - aplikace pro přijímací řízení.

4.2.3.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena na 5 - 40 let podle typu agendy v souladu se Spisovým a skartačním řádem. Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.3.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny s ostatními pracovníky školy.

4.2.3.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.3.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.3.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.3.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání
- Validace
- Používání
- Předávání
- Nahlížení

4.2.3.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje jsou poskytovány třetím osobám – CZVV.

4.2.3.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.3.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.3.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.4 AGENDA VÝCHOVNÉHO PORADCE A ŠKOLNÍHO METODIKA PREVENCE

Jednání s žáky a rodiči, pedagogy, řešení kázeňských problémů, prevence rizik, chování, zpracování metodik, plánů pedagogické podpory, spolupráce, zpracování individuálních studijních plánů.

4.2.4.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele byl dentifikován externí subjekt BAKALÁŘI.

4.2.4.2 ÚČEL ZPRACOVÁNÍ

Evidence a zpracování údajů v oblasti školních činností.

4.2.4.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - klienti / zákazníci
  - jiné osoby: zmocněnci, rodinní příslušníci, žadatelé, stěžovatelé
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - datum narození
  - email
  - telefon
  - adresa

4.2.4.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca 20 měsíčně. Jedná se o zpracování systematické.

4.2.4.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů:

- zdravotní stav.

Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.4.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace je použita;
- Generalizace jepoužita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikacích E-spis LITE ICZ, BAKALÁŘI.

4.2.4.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena po dobu 5 - 10 let v souladu se Spisovým a skartačním řádem. Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.4.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny s ostatními pracovníky školy.

4.2.4.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.4.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.4.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.4.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Sběr
- Uchovávání
- Validace
- Používání
- Předávání
- Nahlížení

4.2.4.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje jsou poskytovány třetím osobám – .

4.2.4.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.4.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.4.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.5 ŠKOLNÍ AKCE A ZÁJEZDY

Zpracování seznamu účastníků školní akce, zveřejňování výsledků a umísťování soutěžících, stanovení podmínek akce, poučení BOZP, kontakty na rodiče, komunikace, uzavírání pojištění, organizace soutěží a akcí.

4.2.5.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. Účel zpracování

Evidence a zpracování údajů v oblasti školních činností.

4.2.5.2 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
    - zaměstnanci
    - klienti / zákazníci
    - jiné osoby: zmocněnci, rodinní příslušníci, žadatelé, stěžovatelé
- kategorie osobních údajů:
    - titul
    - jméno
    - příjmení
    - datum narození
    - email
    - telefon
    - adresa
    - podpis
    - adresa školy
    - bankovní spojení
    - umístění v soutěži

4.2.5.3 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca 1 000 ročně. Jedná se o zpracování systematické.

4.2.5.4 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů – zdravotní stav.

Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.5.5 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikacích E-spis LITE ICZ, BAKALÁŘI.

4.2.5.6 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena po dobu konání akce + 5 let v souladu se Spisovým a skartačním řádem. Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.5.7 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny s ostatními pracovníky školy.

4.2.5.8 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.5.9 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.5.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.5.11 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Sběr
- Uchovávání
- Validace
- Používání
- Předávání
- Nahlížení

4.2.5.12 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje nejsou poskytovány třetím osobám.

4.2.5.13 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.5.14 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.5.15 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.6 PROJEKTOVÁ ČINNOST

Řízení a realizace projektů, příprava žádosti, podkladů k uzavření smluv, komunikace s partnery, s poskytovatelem, pořizování podkladů pro vyúčtování a udržitelnost projektů, podklady pro materiály pro orgány kraje.

4.2.6.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele nebyly identifikovány žádné další subjekty.

4.2.6.2 ÚČEL ZPRACOVÁNÍ

Evidence a zpracování údajů o projektech v oblasti školních činností.

4.2.6.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - zaměstnanci
  - klienti / zákazníci
  - jiné osoby: dodavatelé, smluvní partneři, rodinní příslušníci, žadatelé, stěžovatelé
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - datum narození
  - email
  - adresa
  - číslo OP / CP
  - věk
  - podpis
  - číslo bankovního spojení

4.2.6.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca **50 ročně**. Jedná se o zpracování systematické.

4.2.6.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje zvláštní kategorii osobních údajů – zdravotní stav.

Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. Dle našeho názoru v tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.6.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;

- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikacích: E-spis LITE ICZ.

4.2.6.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena po dobu délky trvání projektu, jeho udržitelnosti, podle požadavku poskytovatele dotace v souladu se Spisovým a skartačním řádem. Dle našeho názoru nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.6.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny s ostatními pracovníky školy.

4.2.6.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.6.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.6.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazal (nezpracovává) v rámci automatických procesů.

4.2.6.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Sběr
- Uchovávání
- Validace

- Používání
- Předávání
- Nahlížení

4.2.6.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje nejsou poskytovány třetím osobám.

4.2.6.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.6.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.6.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.7 POJISTNÉ UDÁLOSTI A ÚRAZY

Jedná se o evidenci úrazů dětí i zaměstnanců, řešení pojistných událostí, škod na majetku a zdraví, komunikaci s poškozenými a pojišťovnami, doručování dokumentů.

4.2.7.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele byly identifikovány subjekty:

- Pojišťovny,
- SATUM Czech – na základě rámcové smlouvy s MSK.

4.2.7.2 ÚČEL ZPRACOVÁNÍ

Administrativní úkony spojené s předmětem činnosti organizace.

4.2.7.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
    - zaměstnanci
    - klienti

- jiné osoby: zmocněnci, smluvní partneři, rodinní příslušníci, žadatelé / stěžovatelé
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - rodné číslo
  - datum narození
  - adresa
  - email
  - telefon
  - podpis

V rámci scénáře je v kategorii zvláštních osobních údajů zpracováván zdravotní stav.

4.2.7.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti spojené s činností zařízení. Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.

Rozsah zpracování je nahodilý, závisí na počtu událostí.

4.2.7.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje ve zvláštní kategorii osobních údajů - zdravotní stav. Subjektu údajů nejsou poskytovány informace, poskytování informací není povinné. Dle našeho názoru v tomto scénáři škola plní s ohledem na právní základ své informační povinnosti v souladu s GDPR.

4.2.7.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace je použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;

- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- listinné podobě
- kancelářských aplikacích
- v aplikacích: elektronické spisové službě espis Lite, FAMA+, InspIS DATA (systém pro sběr a vyhodnocení dat České školní inspekce)

4.2.7.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování trvá po dobu 10 let v souladu se spisovým a skartačním řádem.

4.2.7.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že osobní data jsou v rámci organizace sdílena s dalšími zaměstnanci školy.

4.2.7.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.7.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v centralizovaných systémech.

4.2.7.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

Právo na výmaz je implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazala.

Domníváme se, že v rámci tohoto scénáře zpracování by postačil manuální proces uplatňování a vyřizování žádostí subjektů údajů. Subjekty údajů by měly být informovány, kde svá práva mohou uplatňovat.

4.2.7.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Sběr
- Uchovávání
- Validace, kontrola
- Používání
- Předávání

4.2.7.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři jsou osobní údaje poskytovány dalším subjektům podle charakteru zpracovávané události. Dalšími subjekty jsou

- Pojišťovny
- Česká školní inspekce
- SATUM CZECH s.r.o. (pojišťovací společnost)
- Inspektorát bezpečnosti práce
- Zřizovatel
- PČR

4.2.7.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.7.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.7.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	1	1	2	nízké
ztráta údajů	1	1	2	nízké
pozměňování údajů	1	1	2	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	2	nízké
neoprávněné zpřístupnění uložených údajů	1	1	2	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	2	nízké
neoprávněný přístup k údajům	1	1	2	nízké

4.2.8 PERSONÁLNÍ A PLATOVÁ AGENDA

Jedná se o vedení personální a mzdové agendy u zaměstnanců pracujících na HPP a DPČ. Zpracování reflektuje povinnosti vyplývající ze zákoníku práce. Jsou vedeny údaje o platovém zařazení, platových výměrech, odměňování, mzdách, kvalifikace a jejím prohlubování a zvyšování. Jsou vedeny osobní spisy zaměstnanců a zpracovávány podklady pro materiály pro Radu kraje MSK.

4.2.8.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce.

4.2.8.2 ÚČEL ZPRACOVÁNÍ

Personální a mzdová agenda.

4.2.8.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
    - zaměstnanci

- rodinný příslušník (mj. osoby do 18 let – údaje nutné pro plnění zákonných povinností v rámci mzdové agendy), uchazeč o zaměstnání

- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení
  - datum narození
  - rodné číslo
  - vzdělání
  - email
  - telefon
  - adresa
  - bankovní spojení
  - podpis
  - bezúhonnost
  - mzdové údaje

4.2.8.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem jednak plnění pracovní smlouvy a zejména plnění právní povinnosti dle zákona č. 262/2006 – zákoník práce, zákona č. 586/1992 o daních z příjmů, zákona č. 48/1997 o veřejném zdravotním pojištění, zákona č. 589/1992 o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a dalších závazných norem.

Zpracování se pohybuje zhruba **v rozsahu 60 a více osob měsíčně**. Jedná se o zpracování systematické.

4.2.8.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů obsahuje ve zvláštní kategorii osobních údajů zdravotní stav. Subjektu údajů nejsou poskytovány informace v souladu s článkem 13 Obecného nařízení. Při právním základu postaveném na právní povinnosti záleží na daném kontextu a správce nemusí o existenci tohoto zpracování subjekt údajů informovat, ale obecně nelze považovat platný a účinný právní předpis za apriori zprošťující okolnost pro správce z povinnosti informovat subjekt údajů dle článku 13, resp. 14 Obecného nařízení.

4.2.8.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace je použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;

- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- listinné podobě na sekretariátu školy.
- elektronické podobě v běžných kancelářských aplikacích.
- V aplikacích: elektronická spisová služba e-spis Lite, VEMA.

4.2.8.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování trvá po dobu trvání zaměstnaneckého poměru a následně 50 let po jeho ukončení v souladu vnitřním předpisem – spisový a skartační řád.

4.2.8.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel MGO.

4.2.8.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.8.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v centralizovaných systémech.

4.2.8.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

Právo na výmaz je implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazala.

Domníváme se, že v rámci tohoto scénáře zpracování by postačil manuální proces uplatňování a vyřizování žádostí subjektů údajů. Subjekty údajů by měly být informovány, kde svá práva mohou uplatňovat.

4.2.8.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání

- Validace, kontrola
- Používání
- Předávání
- Nahlížení
- Archivace
- Likvidace

4.2.8.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

OU nejsou předávány třetím osobám.

4.2.8.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.8.15 SEZNAM NESHOD S GDPR

Neshody s GDPR nebyly shledány.

4.2.8.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	2	1	1	nízké
ztráta údajů	2	1	1	nízké
pozměňování údajů	1	1	1	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	1	nízké
neoprávněné zpřístupnění uložených údajů	1	1	1	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	1	nízké
neoprávněný přístup k údajům	1	1	1	nízké

4.2.9 INVENTARIZACE

Provedení dokladových inventur v oblasti pohledávek, závazků, účtu pořizování dlouhodobého majetku, časového rozlišení a ostatních podrozvahových účtů, vyhledávání a kontrola ve smlouvách, účetních a daňových dokladech. Vedení pokladní agendy, účetních a daňových dokladů.

4.2.9.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici správce. V roli zpracovatele nebyly identifikovány žádné další subjekty.

4.2.9.2 ÚČEL ZPRACOVÁNÍ

Kontrola evidence pohledávek a závazků.

4.2.9.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - zaměstnanci
- kategorie osobních údajů:
  - titul
  - jméno
  - příjmení

4.2.9.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem plnění právní povinnosti.

Rozsah zpracování je cca **tisíce ročně**. Jedná se o zpracování systematické.

4.2.9.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů neobsahuje zvláštní kategorii osobních údajů.

Při právním základu postaveném na plnění právní povinnosti nemusí o tomto zpracování subjekt údajů informovat, není třeba udělení souhlasu se zpracováním. V tomto scénáři škola plní své informační povinnosti v souladu s GDPR.

4.2.9.6 POUŽITÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, TECHNIKY ZPRACOVÁNÍ A ULOŽENÍ ÚDAJŮ

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti je zavedena;
- Pravidelná testování jsou prováděna.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- V pomocných kancelářských aplikacích
- V aplikaci IS FAUST - Majetek.

4.2.9.7 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování je stanovena na 10 let v souladu se zákonem o účetnictví. Nastavení doby uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.9.8 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že jsou osobní údaje sdíleny se správci pohledávek, závazků a majetku.

4.2.9.9 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.9.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

MSK má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.9.11 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře nemohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění právní povinnosti.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno pouze vydáním potvrzení o tom, že škola již údaje vymazala (nezpracovává) v rámci automatických procesů.

4.2.9.12 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání
- Validace
- Používání
- Nahlížení

4.2.9.13 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje nejsou poskytovány třetím osobám.

4.2.9.14 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.9.15 SEZNAM NESHOD S GDPR

Zpracování osobních údajů je v souladu s nařízením GDPR.

4.2.9.16 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	2	1	1	nízké
ztráta údajů	2	1	1	nízké
pozměňování údajů	1	1	1	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	1	nízké
neoprávněné zpřístupnění uložených údajů	1	1	1	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	1	nízké
neoprávněný přístup k údajům	1	1	1	nízké
	dopad	**hrozba**	**zranitelnost**	**hodnocení rizika**
náhodné nebo protiprávní zničení údajů	2	1	1	nízké
ztráta údajů	2	1	1	nízké
pozměňování údajů	1	1	1	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	1	nízké
neoprávněné zpřístupnění uložených údajů	1	1	1	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	1	nízké
neoprávněný přístup k údajům	1	1	1	nízké

4.2.10 PŘÍPRAVA A UZAVÍRÁNÍ SMLUVNÍCH VZTAHŮ

Zpracování podkladů pro osoby určené zaměstnancem za účelem uzavření smluv telekomunikačních služeb.

4.2.10.1 ROLE Z HLEDISKA ZPRACOVÁNÍ

Škola je v tomto zpracování v pozici **zpracovatele**. V roli správce byl identifikován externí subjekt – telekomunikační operátor T-Mobile.

4.2.10.2 ÚČEL ZPRACOVÁNÍ

Příprava a uzavírání smluvních vztahů.

4.2.10.3 KATEGORIE SUBJEKTŮ ÚDAJŮ A ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ:

- kategorie subjektů údajů:
  - zaměstnanci
- kategorie osobních údajů:
  - jméno
  - příjmení
  - bydliště
  - číslo bankovního účtu

4.2.10.4 PRÁVNÍ ZÁKLAD, ROZSAH A SYSTEMATIČNOST ZPRACOVÁNÍ

V tomto scénáři zpracování osobních údajů je právním základem udělený souhlas.

Rozsah zpracování se pohybuje cca **10 ročně**. Jedná se o zpracování nesystematické.

4.2.10.5 CHARAKTER OSOBNÍCH ÚDAJŮ A INFORMAČNÍ POVINNOST

Uvedený scénář zpracování osobních údajů neobsahuje zvláštní kategorii osobních údajů. Při právním základu postaveném na udělení souhlasu lze doporučit pro důsledné a kvalitní plnění informační povinnosti způsobem, který je subjektu údajů přístupný, jako vhodné veškerá ujednání o zpracování osobních údajů uvést ve smlouvě nebo v samostatném dokumentu.

Použitá technická a organizační opatření, techniky zpracování a uložení údajů

Užitá technická opatření:

- Pseudonymizace není použita;
- Generalizace není použita;
- Anonymizace není použita;
- Šifrování není použito;
- Obnova dostupnosti není zavedena;
- Pravidelné testy nejsou prováděny.

Užité techniky zpracování:

- Profilování není použito;
- Odvozování není použito.

Uložení osobních údajů týkajících se tohoto zpracování je v:

- Listinné podobě
- Elektronické podobě v aplikacích MS Word a Excel.

4.2.10.6 DOBA ZPRACOVÁNÍ – JAK DLOUHO, ZÁLOHOVÁNÍ, VÝMAZ PO UPLYNUTÍ ÚČELU

Doba zpracování trvá po dobu trvání smlouvy v souladu se Spisovým a skartačním řádem organizace. Doba uchování údajů odpovídá požadavkům stanovených GDPR.

4.2.10.7 INTERNÍ ODPOVĚDNOST A VAZBY

Za tento scénář zpracování osobních údajů odpovídá ředitel školy. Předložená identifikace dokladuje, že osobní data jsou v rámci organizace sdílena mezi pracovníky školy.

4.2.10.8 ŘÍZENÍ INCIDENTU, HLÁŠENÍ

Dle provedené identifikace v tomto scénáři zpracování jsou incidenty řízeny a je stanoven proces eskalace případného porušení zabezpečení údajů.

4.2.10.9 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ BEZ OHLEDU NA PRÁVNÍ ZÁKLAD ZPRACOVÁNÍ

– oprava, přístup, omezení

Škola má tyto procesy zavedeny a dokáže poskytnout přístup nebo opravu údajů individuálně na základě žádosti v rozsahu změny údajů v informačním systému.

4.2.10.10 PROCESY K UPLATŇOVÁNÍ PRÁV SUBJEKTŮ DLE PRÁVNÍHO ZÁKLADU – VÝMAZ, NÁMITKY, PŘENOSITELNOST

V rámci tohoto scénáře mohou být práva výmazu, námitky a přenositelnosti uplatněna, protože se jedná o plnění na základě uděleného souhlasu.

Právo na výmaz by mělo být implementováno automaticky v rámci nastavení doby zpracování, případným žádostem o výmaz by tak mělo být vyhověno vydáním potvrzení o tom, že škola již údaje vymazala a dále je nezpracovává.

4.2.10.11 OPERACE PROVÁDĚNÉ NAD ÚDAJI

- Uchovávání
- Používání
- Předávání

4.2.10.12 POSKYTOVÁNÍ ÚDAJŮ TŘETÍM OSOBÁM – SPOLEČNÍ SPRÁVCI, DŮVĚRYHODNOST ZPRACOVATELŮ, ZPRACOVATELSKÁ SMLOUVA

V tomto scénáři osobní údaje jsou poskytovány třetím osobám – telekomunikačnímu operátorovi

4.2.10.13 PŘEDÁVÁNÍ ÚDAJŮ DO TŘETÍCH ZEMÍ

Údaje nejsou podle výsledků mapování předávány do třetích zemí.

4.2.10.14 SEZNAM NESHOD S GDPR

Nebyly nalezeny neshody s GDPR.

4.2.10.15 ANALÝZA RIZIK

	dopad	hrozba	zranitelnost	hodnocení rizika
náhodné nebo protiprávní zničení údajů	2	1	1	nízké
ztráta údajů	2	1	1	nízké
pozměňování údajů	1	1	1	nízké
neoprávněné zpřístupnění předávaných údajů	1	1	1	nízké
neoprávněné zpřístupnění uložených údajů	1	1	1	nízké
neoprávněné zpřístupnění jinak zpracovávaných údajů	1	1	1	nízké
neoprávněný přístup k údajům	1	1	1	nízké

4.3 INFORMAČNÍ POVINNOST

4.3.1 PLNĚNÍ INFORMAČNÍ POVINNOSTI SPRÁVCE PODLE GDPR

Čl. 12 odst. 1):

„Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby".

Rozsah informací a sdělení, které je správce povinen poskytnout subjektu údajů při získávání osobních údajů, je stanoven:

- v čl. 13 – pokud jsou osobní údaje získány od subjektu údajů;
- v čl. 14 – pokud osobní údaje nebyly získány od subjektu údajů.

V obou článcích jsou stanoveny rovněž podmínky (odst. 4, resp. odst. 5), kdy se informace poskytovat nemusí, nebo poskytují pouze v omezené míře.

4.3.2 MOŽNÉ ŘEŠENÍ INFORMAČNÍ POVINNOSTI PODLE GDPR

Na webových stránkách SŠ, pod odkazem Informace o zpracování osobních údajů budou zveřejněny tyto informace:

- pověřenec pro ochranu osobních údajů:
  - titul, jméno, příjmení;
  - kontaktní údaje.
- osobní údaje jsou v SŠ zpracovávány pouze po nezbytnou dobu, které je individuální pro jednotlivé účely zpracování. Po uplynutí této doby jsou osobní údaje zlikvidovány nebo dále uchovány po dobu stanovenou platným spisovým řádem;

- pokud jsou v SŠ zpracovávány Vaše osobní údaje, máte právo:
    - požadovat od SŠ informaci o zpracování Vašich osobních údajů;
    - požadovat umožnění přístupu k Vašim osobním údajům zpracovávaným v SŠ;
    - požadovat opravu nepřesných osobních údajů (pokud se domníváte, že Vaše osobní údaje zpracovávané SŠ jsou nepřesné);
    - požadovat vymazání Vašich osobních údajů zpracovávaných SŠ, popřípadě požadovat omezení jejich zpracování v souladu s příslušným právním základem pro zpracování osobních údajů;
    - vznést námitku proti zpracování osobních údajů SŠ;
    - požadovat přenositelnost osobních údajů, které jste poskytl (poskytla) SŠ;
    - podat stížnost dozorovému orgánu.
- pokud je zpracování Vašich osobních údajů podmíněno Vaším předchozím souhlasem se zpracováním, máte právo souhlas odvolat. Tím však není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním;
- Svá práva vůči SŠ uplatňujte cestou pověřence pro ochranu osobních údajů.

V souvislosti s uveřejněním kontaktu na pověřence pro ochranu osobních údajů patří k dobré praxi umístit odkaz na pověřence také již na frontpage webu, aby subjekt údajů měl snadnou možnost navázat komunikaci.

4.3.3 DOPORUČUJEME DALŠÍ INFORMACE DLE ČL. 13 GDPR, ZEJMÉNA:

- účely zpracování, pro které jsou osobní údaje určeny;
- právní základ pro zpracování;
- veřejné zájmy SŠ (pokud jsou osobní údaje zpracovávány v rámci tohoto právního základu – například nahrávání telefonních hovorů, využití personalizovaných čipových karet, monitoring služebních vozidel atd.);
- případné příjemce nebo kategorie příjemců osobních údajů (i v třetích zemích);
- zda bude docházet k automatizovanému rozhodování, včetně profilování, a tedy předpokládaným významným důsledkům takového zpracování pro subjekt údajů.

Poskytovat přiměřenou formou (písemně na již zavedených formulářích nebo samostatných formulářích, v elektronické formě na webových stránkách SŠ) s přihlédnutím na konkrétní účel zpracování a skutečnost, zda subjekt údajů těmito údaji ještě disponuje či nikoli.

Pokud jsou osobní údaje získávány jiným způsobem než od subjektů údajů, je nutné posoudit relevanci poskytovaných informací a sdělení s ohledem na zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů. V této souvislosti poukazujeme na:

- lhůty poskytnutí informací uvedené v článku 14, odst. 3 GDPR, a
- možnosti omezení poskytování informací dle článku 14, odst. 5 GDPR.

4.4 STAV ZPRACOVATELSKÝCH SMLUV

Cílem této analýzy bylo posoudit současný stav smluv se zpracovateli, kteří pro SŠ zpracovávají osobní údaje ve vztahu k požadavkům GDPR.

Jak podle současné právní úpravy, tak podle nařízení EU má správce údajů povinnost uzavřít se zpracovatelem, kterého pověří zpracováním údajů, smlouvu o zpracování osobních údajů.

Smlouva o zpracování osobních údajů musí zahrnovat následující:

- zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- přijme všechna opatření požadovaná podle článku 32;
- dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;
- zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;
- je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;
- v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;
- poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

Správce a zpracovatel budou také muset přijmout vhodná technická a organizační opatření, aby zajistili potřebnou úroveň zabezpečení osobních údajů odpovídající danému riziku – mezi tato budou spadat např. pseudonymizace a šifrování osobních údajů, zajištění důvěrnosti, integrity, dostupnosti a odolnosti systémů (vč. zálohování dat), antivirová ochrana, autentizační procesy, omezení přístupových práv apod. V případě porušení zabezpečení osobních údajů bude správce také povinen incidenty ohlašovat Úřadu a v případě vysokého rizika i samotným subjektům údajů, to vše bez zbytečného odkladu (Úřadu, pokud možno do 72 hodin).

Je doporučeno provést revizi všech smluv se zpracovateli a v případě poskytování zpracovatelských služeb se správci a vytvořit dodatek nebo uzavřít samostatnou smlouvu o zpracování osobních údajů.

Pro revizi smluv doporučujeme použít následující kritéria:

- smlouva obsahuje pokyny týkající se ochrany údajů, zacházení s údaji, opatření pro zabezpečení údajů a účely zpracování údajů;
- smlouva zahrnuje zajištění zničení dat po ukončení smlouvy nebo po skončení zpracování;
- smlouva zahrnuje povinnost zachovávat tajemství údajů během i po ukončení smlouvy nebo po zpracování;
- smlouva zahrnuje pravidla pro subdodavatele pro zpracování;
- smlouva zahrnuje smluvní pokuty při incidentech zpracování;
- smlouva zahrnuje právo na audit zpracování osobních údajů;
- smlouva zahrnuje povinnosti týkající se spolupráce při zpracování, auditu a informací správce.

Vzhledem k tomu, že definice zpracování (osobních údajů) byla v GDPR oproti zákonu o ochraně osobních údajů rozšířena i o **nahlédnutí** či **jakékoliv zpřístupnění, je nutné nastavit nově systém tak,** aby kterýkoliv smluvní partner, který sice s osobními údaji nijak nenakládá, ale nelze při plnění předmětu smlouvy vyloučit jeho nahlédnutí na osobní údaje (při servisním zásahu, upgrade systému atd.), byl považován za zpracovatele ve smyslu GDPR a aby správce s takovým zpracovatelem uzavřel písemnou smlouvu obsahující náležitosti dle čl. 28 GDPR.

4.5 PŘIJATÁ TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

K zajištění ochrany osobních údajů jsou v SŠ realizována dále uvedená technickoorganizační opatření:

- Organizační řád – aktualizace
- Pracovní smlouva – aktualizace
- Směrnice o ochraně osobních údajů – nová v souladu s GDPR

4.6 PERSONÁLNÍ BEZPEČNOST

- pravidla personální bezpečnosti jsou zakotvena zejména ve vnitřních směrnicích SŠ a Organizačním řádu;
- pravidla personální práce jsou zakotvena ve vnitřních předpisech;
- pravidla ochrany osobních údajů stanoví interní předpis Směrnice o ochraně osobních údajů;
- noví zaměstnanci (nebo stávající zaměstnanci při změně pracovního místa) procházejí zkušební dobou či adaptačním procesem, v rámci kterého jsou seznamováni se základními vnitřními řídícími směrnicemi a s dalšími předpisy, vztahujícími se k jejich práci;
- pro každé pracovní místo je zpracována Náplň práce zaměstnace obsahující veškeré činnosti, povinnosti, práva a odpovědnosti vztahující se k pracovnímu místu;
- je zaveden systém vzdělávání a odborného rozvoje SŠ – Plán dalšího vzdělávání;
- u SŠ je zaveden proces hodnocení zaměstnanců;

- zaměstnanci mají stanovenu povinnost zachovávat mlčenlivost o skutečnostech, o nichž se dověděli při výkonu svého povolání, která je zakotvena v pracovní smlouvě.

4.7 FYZICKÁ BEZPEČNOST

Fyzickou bezpečnost upravuje obecně Směrnice o ochraně osobních údajů.

4.8 ADMINISTRATIVNÍ BEZPEČNOST

MGO pracuje podle standardní klasifikace informací:

- neveřejné (důvěrné) informace:
    - osobní údaje;
    - citlivé údaje ve smyslu zákona o ochraně osobních údajů;
    - citlivé informace (údaje ekonomické, obchodní, služební apod.).
- veřejné informace (informace, které lze poskytnout na základě zákona o svobodném přístupu k informacím)
- duševní vlastnictví SŠ:
    - zaměstnanecká díla, užitné vzory, vynálezy apod., které jsou podstatné pro činnost SŠ a nejsou všeobecně známé nebo snadno dostupné;
    - výzkumné záměry a projekty, vědeckovýzkumné projekty;
- v SŠ byly vydány vnitřní předpisy o nakládání s dokumenty stanovující pravidla spisové služby ve smyslu zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, v platném znění a jeho prováděcích vyhlášek ve všech procesech nakládání s dokumenty v SŠ, včetně stanovení povinností konkrétním zaměstnancům, zabezpečujícím v SŠ spisovou službu.

Spisový řád a Spisový a skartační plán (Skartační rejstřík) stanovuje skartační znaky a skartační lhůty pro jednotlivé druhy dokumentů.

Perspektivně lze revidovat právní opodstatnění pro délku doby uchovávání osobních údajů a podle potřeby ji upravit ve spisovém a skartačním řádu.

4.9 BEZPEČNOST IT APLIKACÍ A SYSTÉMŮ

SŠ dosud nemá implementován ISMS normu dle ISO 27001 zajišťující bezpečnost informací. Není stanoven proces zjištění a řízení rizik v oblasti IT. S ohledem na rozsah zpracovávaných informací a rozsah technické infrastruktury a v souladu s technickými, personálními a ekonomickými kapacitami je nutné, aby zřizovatel SŠ poskytl vzorovou směrnici pro bezpečnost IT v příspěvkových organizacích, ve které by bylo řešeno řízení přístupů, ukládání zpracovávaných informací, ochrana proti zranitelnosti a zálohování.

p.č.	Neshoda s GDPR	Obsah neshody
4.	článek 32, 1 a)	Zvýšit míru ochrany dat v úložištích pomocí šifrování a pseudonymizace tam, kde to je možné
5.	článek 32, 1 b)	Tam, kde to aplikace umožňují, nastavit systém logování a auditování
6.	článek 32, 1 b)	Zvážit nasazení ISMS systému pro zajištění bezpečnosti dat například implementací normy ISO 27001 a to nejen z hlediska zájmů subjektů údajů, ale i ve vlastním zájmu Organizace.
7.	článek 32, 1 c)	Prakticky žádná z aplikací nemá zajištěný Disaster recovery plán. GDPR jasně hovoří o obnově dostupnosti údajů.
8.	článek 32, 1 d)	Prakticky žádná z aplikací není testována na zranitelnosti a případné incidenty nejsou vyhodnocovány.
9.	článek 20, 1	Prakticky všechny aplikace umožňují export dat, respektive údajů a data mohou být odesílána v některých případech mimo systém. Doporučujeme minimalizovat tyto přístupy, případně zvážit nasazení DLP systému.
10.	článek 13, 2b)	Systémy nejsou připraveny pro vykonávání práva subjektů na portabilitu dat.

Dané požadavky není MGO v současném stavu odborně, personálně a ani materiálně zajistit. Lze konstatovat, že stávající systém dosud zajišťoval plnou ochranu všech zpracovávaných dat.

4.10 OPATŘENÍ PRO LIKVIDACI OSOBNÍCH ÚDAJŮ

Jednou ze základních zásad zpracování osobních údajů dle GDPR je povinnost k uložení osobních údajů ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Jedná se o princip minimalizace dat.

U všech dokumentů obsahujících OÚ jsou stanoveny prostřednictvím Spisového řádu skartační lhůty. V současnosti je tento problém řešen prováděním skartačního řízení a v souladu se skartačními znaky a skartačními lhůtami jsou příslušné dokumenty buď přesunuty do archivu, nebo nevratně likvidovány. Skartace fyzická je pak prováděna na specializovaném zařízení, nebo jsou materiály umístěny do speciálního skartačního boxu OZO.

Zajistit absolutní likvidaci osobních údajů uložených v elektronické podobě je problémem, který stojí mimo rámec technických možnosti MGO. Pokud nebude nastavena automatická skartace, je třeba tento proces realizovat individuálně.

4.11 DOPORUČENÍ PRO PLNĚNÍ POVINNOSTÍ SPRÁVCE PŘI ZABEZPEČENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V ROZSAHU POŽADAVKŮ ČL. 32GDPR

Provedení „datového auditu" – definovat a vymezit to, co má být zabezpečeno. Viz Identifikovaná zpracování.

Pro identifikaci všech míst zpracování osobních údajů bylo analyzováno následující portfólio:

U strukturovaných dat zpracovávaných v aplikacích nebo informačních systémech důsledně zmapovat životní cyklus zpracovávaných osobních údajů do přehledného formátu s cílem stanovit:

- zdroj osobních údajů nebo zdrojový systém osobních údajů (název aplikace / IS);
- účel aplikace / IS;
- rozsah zpracovávaných osobních údajů, pokud není možné stanovit přesný rozsah tak alespoň kategorie zpracovávaných osobních údajů;
- právní základ zpracování osobních údajů;
- doba uchování osobních údajů / skartační lhůta (nejlépe je stanovit ji jako časový interval od pořízení osobních údajů);
- příjemce osobních údajů;
- vlastníka aplikace (business garanta);
- technologické prostředky, na nichž ke zpracování dochází.

nestrukturovaných dat uložených na uživatelských počítačích, sdílených discích, zpracovávaných v emailech atd. byly hodnoceny následující kategorie:

- rozsah, účel a právní základ pro zpracování;
- doba uchování;
- pravidla pro výmaz;
- pravidla pro případné sdílení dat;
- případné příjemce;
- pravidla pro zajištění odpovídající bezpečnosti;
- pravidla pro předávání osobních údajů prostřednictvím elektronické pošty,
- pravidla pro předávání zvláštních kategorií osobních údajů prostřednictvím elektronické pošty;

- technologické prostředky, na nichž ke zpracování dochází (identifikace konkrétního uživatelského počítače nebo notebooku);

Zpracovávat OU je možno jen na zařízeních v majetku školy.

Doporučujeme provést hodnocení rizik na základě hodnocení důvěrnosti, integrity a dostupnosti osobních údajů. Pro hodnocení doporučujeme použít například metodiku hodnocení rizik zákona o kybernetické bezpečnosti.

4.12 KONTROLNÍ ČINNOST

Obecně vyplývá povinnost vedoucích zaměstnanců ke kontrolní činnosti z odpovědnosti za řízení a měli by tedy provádět kontrolu v rozsahu své pravomoci a odpovědnosti jako součásti své řídící práce v souladu s obecně závaznými právními předpisy a vnitřními řídícími akty. Kontrolní činnost SŠ je obecně upravena Vnitřním řádem. Kontrolní činnost je prováděna prostřednictvím interního auditu v rámci plánů kontrolní činnosti.

SŠ má stanoven rozsah kontrolní činnosti zaměřené na zpracování a ochranu osobních údajů ve Směrnici o ochraně osobních údajů. V rámci analýzy nebyly zkoumány konkrétní skutečnosti v případné realizaci provádění kontrolní činnosti.

Řízením kontrolní činnosti zaměřené na plnění požadavků GDPR doporučujeme pověřit pověřence pro ochranu osobních údajů, provádění kontrolní činnosti jako takové je povinností vedoucích zaměstnanců. Doporučujeme zvážit možnost zavedení automatizovaného nástroje na vyhodnocování bezpečnostně-relevantních událostí.

Kontrolní činnost doporučujeme zaměřit na:

- manipulaci s dokumenty obsahujícími osobní údaje (osobní spisy zaměstnanců, klientské informace, ostatní písemnosti) se zaměřením na jejich ukládání do úschovných objektů nebo určených prostor a uzamykání těchto úschovných objektů a prostor;
- zabezpečení počítačů v nepřítomnosti zaměstnance (odhlášení uživatele);
- dodržování pravidel nakládání s přihlašovacími údaji (hesla, PIN apod.);
- aktuálnost záznamů o činnostech zpracování;
- realizaci technických a organizačních opatření minimálně v tomto v rozsahu:
    - přezkoumání přístupových oprávnění uživatelů a administrátorů;
    - kontrolu auditních záznamů o přístupech k osobním údajům (zejména oprávněnost přístupů);
    - kontrolu záloh na páskách (čitelnost, obnova dat);
    - legálnost a správnost instalovaného SW;
    - kontrola ošetření technických zranitelností útvarem informačních technologií.

- kontrolní činnost provádět průběžně, ale tak aby alespoň 1 x ročně byl zkontrolován celý rozsah zpracování osobních údajů.

5. NÁVRHY ŘEŠENÍ

V následujíc části analýzy jsou rozebrány rozhodující procesy pro realizaci požadavků GDPR. Problematika je dělena do několika oblastí, od úpravy směrnic, přes ustavení pověřence pro ochranu osobních údajů, povinnosti o vedení záznamů o činnosti zpracování až po návrhy jednotlivých procesů definovaných GDPR. Za klíčové operace lze považovat:

1. Upravit existující Směrnici o ochraně osobních údajů a zahrnout do ní informace kde a jak mohou subjekty údajů uplatnit svá práva a informovat subjekty údajů spadajících do kategorie zaměstnanců o tom, v jakých scénářích a procesech jsou v rámci SŠ jejich data zpracovávána.
2. Zkontrolovat stávající Směrnici upravující skartační řád stanovující pravidla skartace a archivace v závislosti na typu dokumentu, jeho klasifikaci a retenční době údajů.

5.2 POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Povinnost jmenovat pověřence pro ochranu osobních údajů stanoví článek 37 odst. 1 písm. b) GDPR, podle kterého „Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;".

SŠ jako orgán veřejné moci má zákonnou povinnost vyplývající z nařízení GDPR stanovit pověřence pro ochranu osobních údajů – zajistí zřizovatel do 18. 5. 2018

5.3 POSTAVENÍ POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Podle čl. 38 GDPR „Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů".

Je tedy důležité, aby pověřenec byl zapojen co nejdříve do všech záležitostí týkajících se ochrany osobních údajů, a to již ve fázi implementace GDPR. Z tohoto důvodu:

- pověřenec by měl mít možnost pravidelného přístupu ke konzultacím s vyšším a středním managementem, nebo by měl být alespoň neprodleně obeznámen s výstupy porad managementu, které mohou mít vztah k ochraně osobních údajů;
- jeho přítomnost by měla být vyžadována vždy tam, kde se přijímají rozhodnutí s dopadem do ochrany osobních údajů. Pověřenec musí obdržet všechny podstatné informace, aby mohl poskytnout odpovídající radu;
- stanovisku pověřence musí být přiznána patřičná závažnost. V případě, že názory či rady pověřence nebyly akceptovány, měly by být zdokumentovány důvody jejich nepřijetí;

- pověřenec musí být informován v případě porušení zabezpečení ochrany osobních údajů nebo jiné, s ochranou osobních údajů související události;

Mezi důležité dovednosti a zkušenosti pověřence patří:

- znalost národního a unijního práva v oblasti ochrany dat a praktické zkušenosti včetně znalosti GDPR;
- znalost prováděných zpracovatelských operací v SŠ;
- znalost informačních technologií a bezpečnosti dat;
- znalost vnitřních procesů a specifik SŠ;
- schopnost propagovat kulturu ochrany dat v SŠ.

5.4 DOPORUČENÍ PERSONÁLNÍHO OBSAZENÍ

Roli pověřence musí vždy vykonávat fyzická osoba – zajistí zřizovatel do 18. 5. 2018.

5.5 VLASTNÍ ZAMĚSTNANEC

Pokud je pověřencem jmenován vlastní zaměstnanec, neznamená to, že musí celý fond pracovní doby věnovat pouze povinnostem pověřence, tj. může to být jedna z více povinností takového zaměstnance. Pověřenec však nemůže zastávat pracovní místo, na kterém by stanovoval účely a prostředky zpracování osobních údajů. Typickým příkladem konfliktního postavení uvádí WP29 pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), příp. pozice na nižším stupni organizační struktury, pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování.

Výhodou tohoto řešení je, že vlastní zaměstnanec zná vnitřní procesy a specifika SŠ, možnou nevýhodou může být neznalost či neorientování se v problematice ochrany osobních údajů, menší přehled v rámci existujících řešení.

5.6 EXTERNISTA NA ZÁKLADĚ SMLOUVY O POSKYTOVÁNÍ SLUŽEB

Externího pověřence pro ochranu osobních údajů může zabezpečovat i právnická osoba za předpokladu, že funkci samotnou reálně vykonává fyzická osoba. Výhody a nevýhody tohoto řešení jsou opačné ve srovnání s předcházející variantou, jelikož externista nezná detailně vnitřní procesy a specifika SŠ, naopak podrobně zná problematiku ochrany osobních údajů a obvykle má díky většímu záběru širší přehled.

5.6.1 VLASTNÍ ZAMĚSTNANEC S EXTERNÍ PODPOROU

Možným řešením je také jmenovat vlastního zaměstnance s podporou poradenské firmy specializující se na tuto problematiku.

Tato varianta v podstatě slučuje výhody obou předchozích variant a eliminuje jejich nevýhody.

Shrnutí a doporučení k popsaným alternativám DPO:

SŠ nemusí jmenovat pověřence pro ochranu osobních údajů, protože není orgánem veřejné moci a neprovádí rozsáhlá zpracování osobních údajů. Pro přechodné období bude MGO využívat pověřence svého zřizovatele – Moravskoslezského kraje prostřednictvím krajského úřadu. Výhodou takového řešení je znalost vnitřních procesů a specifik SŠ.

5.7 NÁVRH KATALOGU ČINNOSTÍ POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

V etapě implementace navrhovaných opatření:

- Rozpracovat koncepci (politiku) zpracování a ochrany osobních údajů do platných vnitřních předpisů SŠ v odlišnostech od opatření implementovaných v souvislosti se zákonem o ochraně osobních údajů.
- Zavést opatření pro vedení záznamů o činnostech zpracování.
- Podílet se na řízení a vyhodnocování realizace implementačního plánu a verifikaci souladu jednotlivých implementovaných opatření.
- Proškolit vybrané zaměstnance SŠ ke změnám v souvislosti s přechodem k GDPR.

Po implementaci opatření GDPR:

- Pro zabezpečení komunikace zajišťovat zejména:
    - kontaktní místo pro subjekty údajů (v rámci i mimo SŠ);
    - komunikaci s dozorovým úřadem, zpracovateli, jinými správci a třetími stranami, včetně dozorových úřadů cizích zemí.
- V rámci trvalého monitoringu souladu s GDPR a dalšími souvisejícími právními předpisy upravujícími ochranu osobních údajů zejména:
    - ověřovat relevantnost vyhodnocení rizik pro práva a svobody subjektů údajů pro prováděné zpracovatelské operace;
    - podílet se na testování účinnosti přijatých technických a organizačních opatření a připravovat návrhy nezbytných změnových řízení;
    - v součinnosti s odpovědnými zaměstnanci SŠ:
        - hodnotit efektivitu a účinnost přijatých organizačních a technických opatření a připravovat nezbytná změnová řízení,
        - řídit výkon práv subjektů údajů a zajišťovat jejich informovanost o průběhu a řešení jejich požadavku na uplatnění práva do stanovené lhůty.
    - v součinnosti s vedením SŠ zajistit:

        - ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu;
        - oznamování případů porušení zabezpečení osobních údajů subjektu údajů.
    - dokumentovat všechny případy porušení zabezpečení osobních údajů;
    - řídit kontrolní činnost zaměřenou na zpracování a ochranu osobních údajů v SŠ i u zpracovatelů.
- Při dohledu nad zpracovatelskými operacemi:
    - vést a dle potřeby aktualizovat záznamy o činnostech zpracování;
    - při vzniku potřeby nové zpracovatelské operace, nebo změny již existující, připravit návrh procesů a podklady k rozhodnutí vedení SŠ související s:
        - dodržením zásad zpracování osobních údajů a zvláštních kategorií osobních údajů uvedených v čl. 5 – 11 GDPR;
        - přípravou smlouvy o zpracování osobních údajů v případě, že zpracovatelskou operaci nebo její část bude provádět zpracovatel;
        - vyhodnocovat rizika pro práva a svobody subjektů údajů:
            - v případě, že riziko bude vyhodnoceno jako vysoké, posoudit právní základ nového zpracování a vyjádřit se k nutnosti zda provést či neprovést posouzení vlivu na ochranu osobních údajů;
            - v případě kladného vyjádření ve spolupráci s odpovědnými zaměstnanci SŠ provést posouzení vlivu zamýšlené operace zpracování na ochranu osobních údajů a případně zahájit konzultační činnost s dozorovým úřadem;
            - o rozhodnutí dozorového úřadu neprodleně informovat vedení SŠ.
        - požadavky na zabezpečení osobních údajů.
    - při zániku zpracovatelské operace, nebo jakékoli její části, připravit návrh procesů a podklady pro rozhodnutí správce, související s:
        - dobou uchování osobních údajů za účelem archivace, pokud není určena platným skartačním plánem;
        - rozsahem a typy osobních údajů, které budou pro případnou archivaci uchovány.
- Rozvíjet znalosti a provádět vzdělávání zaměstnanců SŠ zpracovávajících osobní údaje v problematice ochrany osobních údajů;
- Poskytovat poradenství a informace vedení SŠ, a to zejména:
    - formou helpdesku na vyžádání;
    - formou trvalého monitoringu informací z dostupných zdrojů (stanoviska dozorového úřadu a evropských orgánů, judikáty, rozhodovací praxe atd.), jejich následného vyhodnocení a předání návrhů pro případné zlepšení či aktualizaci;
    - formou ad hoc konzultací s dozorovým úřadem.

5.8 ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Záznamy o činnostech zpracování jsou určeny k doložení souladu s GDPR, a to jak z pozice správce, tak i z pozice zpracovatele.

Záznamy o činnostech zpracování:

- se vyhotovují písemně, počítaje v to i elektronickou podobu,
- na požádání se předkládají dozorovému úřadu.

5.9 ZÁZNAMY O ČINNOSTECH VEDENÉ SPRÁVCEM

Záznamy o činnostech zpracování musí obsahovat:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů;
- účely zpracování;
- kategorie subjektů údajů;
- kategorie osobních údajů;
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, vč. příjemců ve třetích zemích nebo mezinárodních organizacích;
- identifikace třetí země (mezinárodní organizace), které jsou případně předány osobní údaje;
- vhodné záruky v případě předání osobních údajů do třetí země (mezinárodní organizaci) podle čl. 49 odst. 1 druhého pododstavce GDPR;
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1. GDPR (i u případného zpracovatele, pokud se na zpracování podílí).

Nad rámec uvedených povinných údajů v záznamech o činnostech zpracování podle čl. 30 odst. 1 GDPR je nadále nutné uvádět také právní základ zpracování podle čl. 6 GDPR, a to včetně příslušných právních předpisů, pokud je tímto právním základem „plnění právní povinnosti".

5.10 ZÁZNAMY O ČINNOSTECH VEDENÉ ZPRACOVATELEM

Záznamy o činnostech zpracování musí obsahovat:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů;
- kategorie zpracování prováděného pro každého ze správců;
- identifikace třetí země (mezinárodní organizace), které jsou případně předány osobní údaje;

- vhodné záruky v případě předání osobních údajů do třetí země (mezinárodní organizaci) podle čl. 49 odst. 1 druhého pododstavce GDPR;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1. GDPR.

5.11 NÁVRH PROCESŮ K HLÁŠENÍ NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

Zjištění bezpečnostní události

- Hlášení bezpečnostní události nebo incidentu odpovědné osobě nebo pověřenci pro ochranu osobních údajů;
- vyhodnocení zdroje informace o narušení (interní, externí atd.);
- vyhodnocení základních informací;
- rozhodnutí o klasifikaci (událost nebo incident).

Reakce na bezpečnostní události a incidenty

- Událost:
    - odpovědná osoba/pověřenec pro ochranu osobních údajů událost vyšetří;
    - konfrontace události s historií událostí (opakovaná nebo nahodilá událost);
    - návrh opatření k nápravě;
    - ukončení šetření události.
- Incident:
    - svolání odpovědných osob souvisejících s řešením incidentu;
    - pokud je možné, tak realizace okamžité nápravy (zastavení provozu, zablokování práv atd.);
    - identifikace typu osobních údajů, u kterých došlo k porušení bezpečnosti;
    - přibližný rozsah údajů;
    - identifikace pravděpodobného zdroje úniku, narušení;
    - popis pravděpodobných důsledků dopadů na subjekty údajů;
    - vyhodnocení rizika dopadů na práva a svobody subjektů údajů:
        - bez rizika;
        - riziko;
        - vysoké riziko.
    - kontaktování odpovědné osoby z vedení SŠ;
    - rozhodnutí v případě vyhodnocení:

- rizika - ohlášení dozorového úřadu;
- vysokého rizika - ohlášení dozorového úřadu a oznámení subjektům údajů.

  - návrh nebo přijatá nápravná opatření k snížení dopadů na práva subjektů údajů,
  - návrh nebo přijatá nápravná opatření k eliminaci příčiny porušení bezpečnosti osobních údajů,
  - zpracování a odeslání hlášení dozorovému úřadu podle výše vyhodnoceného rizika.

5.11.1 Řešení bezpečnostního incidentu

- další vyšetřování incidentu na základě návrhů uvedených v hlášení dozorovému úřadu,
- návrh a přijetí dalších nápravných opatření,
- kontrola účinnosti přijatých opatření.

Nutno vypracovat jako součást Směrnice o ochraně osobních údajů

5.12 Návrh rozhodovacího procesu při uplatňování práv subjektů údajů

5.12.1 Právo být informován o zpracování osobních údajů

Právo být informován o zpracování osobních údajů – rozumí se právo subjektu na určité informace o zpracování jeho osobních údajů. Jde zejména o informace o účelu zpracování, totožnosti správce, o jeho oprávněných zájmech, o příjemcích osobních údajů. Jedná se o tzv. pasivní právo, jelikož aktivitu musí vůči subjektu údajů vyvinout správce, aby požadované informace stanovené v GDPR subjektu údajů poskytl (při shromažďování osobních údajů od subjektu údajů – viz čl. 13 GDPR), resp. zpřístupnil (v případě, že osobní údaje nebyly získány od subjektu údajů – viz čl. 14 GDPR).

5.12.1.1 Návrh rozhodovacího procesu:

- Pokud jsou osobní údaje shromažďovány od subjektu údajů:
  - posoudit, vzhledem k účelu zpracování, pro který účel jsou osobní údaje shromažďovány, které informace dle § 13 GDPR je nutno subjektu údajů sdělit (informace se sdělit nemusí, pokud subjekt údajů již tyto informace má, a do té míry, v níž je má) a jakým způsobem;
  - sdělit či poskytnout subjektu údajů informace v rozsahu a způsobem dle předchozího odstavce již při shromažďování osobních údajů.
- Pokud osobní údaje nebyly získány od subjektu údajů:
  - posoudit, vzhledem k účelu zpracování, pro který jsou osobní údaje zpracovávány, nutnost poskytnout subjektu údajů informace a jejich rozsah (informace se sdělit nemusí, pokud subjekt údajů již tyto informace má, nebo kdy zaznamenání či zpřístupnění osobních údajů

je výslovně stanoveno právními předpisy, nebo kdy poskytnutí těchto informací subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí) a jako formou (písemně či ústně);

- poskytnout subjektu údajů informace v rozsahu a formou dle předchozího odstavce:
  - v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
  - nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo
  - nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

5.12.2 PRÁVO NA PŘÍSTUP K OSOBNÍM ÚDAJŮM

Právo na přístup k osobním údajům – tímto se rozumí právo získat od správce informaci (potvrzení), zda jsou či nejsou osobní údaje subjektu údajů zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování;
- kategorie dotčených osobních údajů;
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- plánovaná doba, po kterou budou osobní údaje uloženy;
- existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku;
- právo podat stížnost u dozorového úřadu;
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.

5.12.2.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost tazatele, který uplatňuje své právo. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje tazatele v SŠ zpracovávány;
- pokud ano, poskytnout tazateli tuto informaci a současně, pokud to tazatel požaduje, poskytnout informace v požadovaném rozsahu (kopii zpracovávaných údajů), max. však v rozsahu uvedeném v předchozím;
- pokud ne, poskytnout tazateli informaci, že jeho osobní údaje nejsou předmětem zpracování osobních údajů v SŠ.

5.12.3 PRÁVO NA OPRAVU NEPŘESNÝCH OSOBNÍCH ÚDAJŮ

Právo na opravu nepřesných osobních údajů – toto právo neznamená povinnost SŠ aktivně vyhledávat nepřesné údaje (nic tomu však nebrání), ani to neznamená povinnost například každoročně požadovat po subjektu údajů aktualizaci jeho údajů. Pokud se subjekt údajů domnívá, že správce zpracovává jeho nepřesné údaje, upozorní jej na to.

5.12.3.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která uplatňuje právo na opravu údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit skutečný stav (přesnost) dotčených zpracovávaných osobních údajů subjektu údajů;
- dle potřeby vyžadovat od subjektu údajů relevantní doklad stvrzující avizovanou nepřesnost ve zpracování osobních údajů;
- dle doloženého stavu nepřesné zpracovávané osobní údaje opravit.

5.12.4 PRÁVO NA VÝMAZ (BÝT ZAPOMENUT)

Právo na výmaz (být zapomenut) – znamená povinnost správce zlikvidovat osobní údaje, pokud je splněna alespoň jedna podmínka:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování;
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
- osobní údaje byly zpracovány protiprávně;
- osobní údaje musí být vymazány ke splnění právní povinnosti;
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

5.12.4.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která uplatňuje právo na výmaz, tj. zda se skutečně jedná
- o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely a na základě jakého právního důvodu (viz čl. 6 GDPR);
- posoudit nebo vyhodnotit zpracování osobních údajů, kdy je splněna alespoň jedna z uvedených podmínek – u těchto zpracování osobní údaje subjektu údajů zlikvidovat (v listinné i elektronické formě);
- u zpracování, kde nelze uplatnit ani jednu z uvedených podmínek, osobní údaje nelikvidovat.

5.12.5 PRÁVO NA OMEZENÍ ZPRACOVÁNÍ

Právo na omezení zpracování – toto právo lze vnímat jako „právo dočasné". Subjekt údajů může uplatnit toto své právo v případech:

- pokud popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- pokud je zpracování protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

5.12.5.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která uplatňuje právo na omezené zpracování, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda nastala jedna z výše uvedených podmínek pro uplatnění práva;
- pokud bylo zpracování omezeno:
    - mohou být dotčené osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo důležitého veřejného zájmu;
    - je nutno upozornit subjekt údajů, který dosáhl omezení zpracování, na to, že bude omezení zpracování zrušeno.
- Způsoby omezení zpracování osobních údajů:
    - dočasný přesun vybraných údajů do jiného systému zpracování;
    - znepřístupnění vybraných osobních údajů uživatelům;
    - dočasné odstranění zveřejněných údajů z internetových stránek;
    - v systémech automatizovaného zpracování zajistit, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny.

5.12.6 PRÁVO NA PŘENOSITELNOST

Právo na přenositelnost – podstatou uplatnění tohoto práva je možnost za určitých podmínek získat osobní údaje, které se týkají subjektu údajů a které správci poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu, například JSON, CSV, TXT, a právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil. Zároveň má subjekt údajů, pokud požádá, i právo na to, aby správce předal jeho osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu jinému správci, je-li to technicky proveditelné.

Pro uplatnění tohoto práva musí být současně splněny dvě podmínky:

- musí jít o zpracování založené na právním základu souhlasu či smlouvě;
- zpracování se provádí automatizovaně.

5.12.6.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která uplatňuje právo na přenositelnost údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely, na základě jakého právního důvodu (viz čl. 6 GDPR) a v jaké formě (manuální nebo listinná, automatizovaná nebo elektronická);
- pokud jsou splněny společné podmínky uvedeny výše, postupovat podle formulace požadavku subjektu údajů na uplatnění tohoto práva.

5.12.7 PRÁVO VZNÉST NÁMITKU

Právo vznést námitku – subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které jsou zpracovávány na základě právních důvodů:

- zpracování je nezbytné pro plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany.

5.12.7.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která vznáší námitku proti zpracování osobních údajů, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou osobní údaje subjektu údajů v SŠ zpracovávány, pro jaké účely a na základě jakého právního důvodu;
- pokud je zpracování založeno na některém ze dvou právních důvodů uvedených výše, posoudit nebo vyhodnotit, zda existují nebo neexistují závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků;
- v návaznosti na posouzení nebo vyhodnocení skutečností dle předchozího odstavce osobní údaje dále zpracovávat nebo nezpracovávat.

Pozn.: námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nelze již jeho osobní údaje pro tento účel zpracovávat.

Bude implementováno do Směrnice o ochraně osobních údajů

5.12.8 PRÁVO NEBÝT PŘEDMĚTEM AUTOMATIZOVANÉHO INDIVIDUÁLNÍHO ROZHODOVÁNÍ, VČETNĚ PROFILOVÁNÍ

Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování – toto právo zajišťuje subjektu údajů, že nebude předmětem rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká. Automatizované rozhodování je přípustné v případě, kdy je nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, pokud je povoleno právem EU nebo členským státem nebo pokud je založeno na výslovném souhlasu subjektu údajů.

5.12.8.1 NÁVRH ROZHODOVACÍHO PROCESU:

- ověřit totožnost osoby, která uplatňuje toto právo, tj. zda se skutečně jedná o subjekt údajů. Tato povinnost se nevztahuje na případy, kdy je žádost doručena prostřednictvím datové schránky nebo elektronickou poštou podepsanou zaručeným elektronickým podpisem;
- ověřit, zda jsou v SŠ zpracovávány osobní údaje subjektu údajů způsobem, který by byl v rozporu s tímto právem;
- pokud ano, takové zpracování osobních údajů ukončit.

5.12.9 SPOLEČNÁ USTANOVENÍ K ROZHODOVACÍM PROCESŮM

- s výjimkou práva být informován o zpracování osobních údajů musí být informace
- o přijatých opatřeních žadateli (subjektu údajů) poskytnuta bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Lhůtu lze ve výjimečných případech prodloužit o dva měsíce, o čemž musí být subjekt údajů ze strany správce informován, včetně důvodů prodloužení;
- informace, veškerá sdělení a provedené úkony na žádost subjektu údajů se poskytují a činí bezplatně. Pouze v případě, kdy jsou žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď uložit přiměřený poplatek, nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost dokládá správce;
- o zneužití práva subjektem údajů se jedná zejména tehdy, pokud se žádosti opakují a jsou zjevně nedůvodné či nepřiměřené. V takovém případě může správce uložit přiměřený poplatek nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost dokládá správce;
- pokud subjektem údajů požadovaná opatření nebyla správcem přijata, musí správce bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti informovat subjekt údajů o důvodech nepřijetí těchto opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

5.12.9.1 NOVĚ APLIKOVANÉ ADMINISTRATIVNÍ OPERACE NA MGO:

- provést u každého účelu zpracování analýzu rozhodovacího procesu s cílem předem připravit možné odpovědi na žádosti o uplatnění jednotlivých práv (tj. zda žádosti bude vyhověno či nebude, v takovém případě včetně argumentace, proč vyhověno nebude). Tímto de facto vznikne jednoznačné rozhodovací schéma, které umožní pružně reagovat do 1 měsíce i v nepřítomnosti odpovědných osob atp.;
- zavést, a subjektům údajů dát na vědomí, jedno vstupní místo pro žádosti o uplatňování jednotlivých práv (pověřenec pro ochranu osobních údajů, pokud bude tato role zřízena) a vnitřní procesy nastavit tak, aby bylo rovněž jedno výstupní místo zpět k subjektům údajů.

Bude nově součástí Směrnice o ochraně osobních údajů.

5.13 NÁVRH ROZHODOVACÍHO PROCESU PRO REALIZACI POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

5.13.1 NÁVRH ROZHODOVACÍHO PROCESU

- Nově bude nutné na MGO vyhodnotit právní základ zpracování, pro které je nutno případně provést posouzení vlivu na ochranu osobních údajů, a stanovit, zda lze aplikovat ustanovení čl. 35 odst. 10 GDPR, tj. *„Pokud má zpracování podle čl. 6 odst. 1 písm. c)[1] nebo e)[2] právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, odstavce 1 až 7 se nepoužijí, ledaže by členské státy považovaly provedení tohoto posouzení před činnostmi zpracování za nezbytné*". Pokud citované ustanovení GDPR aplikovat lze, posouzení vlivu není nutno provádět;
- pokud citované ustanovení GDPR na MGO aplikovat nelze, zvážit (vyhodnotit), zda je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob[3]. Mezi takové typy operací zpracování mohou patřit ty, při nichž jsou zejména

[1] zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje

[2] zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce

[3] fyzická, hmotná nebo nehmotná újma, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v oSŠorech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů

používány nové technologie, nebo které jsou zcela nového druhu a u nichž správce dosud neprovedl posouzení vlivu na ochranu osobních údajů, nebo které se staly nezbytnými z důvodu času, který uplynul od prvotního zpracování.

- pokud bude úvahou dle předchozího odstavce vyhodnoceno, že:
  - je nepravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, posouzení vlivu na ochranu osobních údajů jako takové není nutno provádět;
  - je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, vyhodnotit zejména pravděpodobnost a závažnost vysokého rizika a zohlednit přitom povahu, rozsah, kontext a účely zpracování a zdroje rizika;
- výsledek konkrétního posouzení bude vždy východiskem při rozhodování o realizaci vhodných (přiměřených) opatřeních, a to včetně dostupnosti vhodných technologií a nákladů na provedení opatření;
- pro soubor podobných operací zpracování, které představují podobné riziko, je dostačující jedno posouzení;
- pro posouzení, zda je nebo není nutné provést posouzení vlivu na ochranu osobních údajů, bude MGO požadovat vyjádření pověřence pro ochranu osobních údajů.

5.13.2 METODIKA PRO PŘÍPADNÉ POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

- Analýza potřebnosti zpracování osobních údajů:
  - MGO pracuje jen s těmi OÚ, které jsou nutné pro zajištění administrativních operací v souvislosti s její činností a posláním
  - odůvodnění potřebnosti zpracování osobních údajů daným způsobem s důrazem položeným na nezbytnost zpracování;
  - posouzení možných dopadů na práva a svobody fyzických osob;
  - doposud realizovaná opatření, která předcházela zpracování osobních údajů.
- Posouzení původu, povahy, zvláštností a závažností rizik při zpracování:
  - organizační rizika při zpracování;
  - technická rizika při zpracování.
- Návrh souboru technických a organizačních opatření pro eliminaci rizik pro dosažení souladu s GDPR:
  - opatření organizačního charakteru;
  - opatření fyzické bezpečnosti;
  - opatření administrativní a personální bezpečnosti;
  - opatření počítačové bezpečnosti;
  - kontrolní činnost;
  - školení zaměstnanců podílejících se na zpracování.

- Návrh povinností osob k zabezpečení ochrany osobních údajů:
    - definice povinností jednotlivých rolí a zaměstnanců při zpracování;
    - zpracování dokumentace včetně vzorů příslušných formulářů (poučení, záznamy atd.).
- Zdůvodnění a posouzení návrhu na zpracování:
    - sumarizace závěrů;
    - stručný popis řešení;
    - provedení testu proporcionality, ve kterém musí oprávněné zájmy správce převažovat nad ochranou soukromí subjektu údajů.

MGO bude nově sledovat vývoj v této oblasti, dostupné informace jsou průběžně zveřejňovány na webových stránkách Úřadu pro ochranu osobních údajů pod základním odkazem „Obecné nařízení EU (GDPR)".

5.14 NÁVRH METODIKY A POSTUPU PRO REALIZACI ZÁMĚRNÉ OCHRANY

„by design"

5.14.1 VZNIK NOVÝCH ZPRACOVATELSKÝCH OPERACÍ NEBO ZMĚNA JIŽ EXISTUJÍCÍCH

- Navrhnout procesy a zpracovat příslušné podklady s cílem zajistit, aby zpracování osobních údajů pro nový či modifikovaný účel bylo v souladu s příslušnými ustanoveními GDPR, zejména:
    - dodržení zásad zpracování osobních údajů dle čl. 5;
    - deklarovat zákonnost zpracování, tj. definovat právní důvod zpracování dle čl. 6;
    - v případě, že právním důvodem zpracování je souhlas subjektu údajů se zpracováním, stanovit podmínky jeho vyjádření, prokazatelnosti a postupů v případě jeho odvolání dle čl. 7;
    - v případě, že budou zpracovávány zvláštní kategorie osobních údajů, zajistit jejich zpracování v souladu s čl. 9, tj. zejména:
        - deklarovat zákonnost zpracování;
        - stanovit právní důvod zpracování.
- V případě, že se na zpracování bude podílet zpracovatel a zmocnění ke zpracování nevyplývá z právního předpisu, před vlastním zpracováním uzavřít se zpracovatelem smlouvu o zpracování osobních údajů. Smlouva musí mít náležitosti dle čl. 28. Smlouva může být uzavřena formou:
    - samostatné smlouvy;
    - příslušná ustanovení mohou být zapracována do jiné smlouvy;
    - dodatku ke smlouvě.
- Vyhodnotit rizika zpracování pro práva a svobody subjektů údajů. V případě, že riziko bude vyhodnoceno jako vysoké, provést posouzení vlivu zamýšlené operace zpracování na ochranu osobních údajů a případně zahájit konzultační činnost s dozorovým úřadem;
- Stanovit požadavky na zabezpečení osobních údajů. Zde se musí vycházet z posouzení rizika zpracování pro práva a svobody subjektů údajů dle předchozího bodu a z analýzy rizik. Je důležité posoudit vhodnost nasazení opatření dle čl. 32 k:
    - pseudonymizaci a šifrování osobních údajů (typicky v případech, kdy externí firma má administrátorská právy k některému IS a může získat přístup k osobním údajům);
    - zajištění důvěrnosti, integrity, dostupnost a odolnosti pracování osobních údajů;
    - obnovitelnosti a zajištění dostupnosti osobních údajů;
    - testování, posuzování a hodnocení účinnosti zavedených bezpečnostních opatření (aby mělo SŠsoustavnou záruku za to, že osobní údaje jsou zpracovávány bezpečně).

5.14.2 ZÁNIK ZPRACOVATELSKÉ OPERACE NEBO JAKÉKOLI JEJÍ ČÁSTI

Navrhnout procesy a zpracovat podklady související s:

- dobou uchování osobních údajů za účelem archivace je určena platným skartačním plánem;
- rozsahem a typy osobních údajů, které budou pro případnou archivaci uchovány;
- způsobem likvidace osobních údajů v elektronické i listinné podobě.

5.15 NÁVRH METODIKY A POSTUPU PRO REALIZACI STANDARDNÍ OCHRANY

„by default"

5.15.1 ZÁKLADNÍ PRAVIDLA FYZICKÉ BEZPEČNOSTI

- požadavky na fyzickou bezpečnost posuzovat v kontextu s opatřeními fyzické bezpečnosti realizovanými v příslušném objektu (areálu, budově). Těmito opatřeními jsou:
    - režimová opatření (vstup a pohyb osob, klíčový režim, návštěvy, provádění úklidu);
    - technické prostředky (mechanické zábranné prostředky a systémy technické ochrany).
- nosiče osobních údajů v listinné i elektronické formě uchovávat způsoby, které zamezí nahodilému či neoprávněnému přístupu k osobním údajům. Možná řešení:
    - použití uzamykacích úschovných objektů (trezory, skříně, kartotéky, kontejnery, …); nebo
    - nosiče ukládat v uzamykacích prostorech s kontrolovaným vstupem pouze oprávněných osob.
- Stanovit režimová opatření (viz výše) ve vztahu k úschovným objektům a prostorům, ve kterých jsou uchovávány nosiče osobních údajů (viz Organizační řád MGO, Provozní řád MGO)

5.15.2 ZÁKLADNÍ PRAVIDLA PERSONÁLNÍ BEZPEČNOSTI

- Výběr vhodných kandidátů na pracovní zařazení s ohledem na vykonávanou práci z hlediska:
    - odborných kvalit;
    - bezúhonnosti.
- Stanovit pravidla pro:
    - příjem nových zaměstnanců – zpracování popisu pracovní náplně, seznámení zaměstnance s pracovními povinnostmi a vnitřními předpisy vztahujícími se k výkonu jeho práce, vstupní školení z hlediska povinností k ochraně informací, přidělení přístupových oprávnění k informacím zpracovávaným v informačních systémech – částečně již zavedeno v rámci vnitřních směrnic;
    - průběh pracovního poměru – periodická a ad hoc školení zaměřena k ochraně informací, reakce na případné změny pracovního zařazení – změna či odebrání přístupových oprávnění do informačních systémů;

- ukončení pracovního poměru – předání agend, za které zaměstnanec odpovídal, odebrání přístupových oprávnění do informačních systémů nejpozději v poslední den trvání pracovního poměru.

5.15.3 ZÁKLADNÍ PRAVIDLA ADMINISTRATIVNÍ BEZPEČNOSTI

- stanovit pravidla klasifikace informací;
- stanovit postupy a pravidla pro manipulaci s dokumenty od jejich doručení, resp. vzniku, až po vyřazení ve skartačním řízení, včetně kontroly a odpovědnosti za výkon těchto činností.

5.15.4 ZÁKLADNÍ PRAVIDLA BEZPEČNOSTI IT

- stanovit odpovídající technická a organizační opatření a tato zdokumentovat. Je třeba vycházet ze závěrů analýzy rizik, která zdůvodní opodstatněnost implementace (ale zejména opodstatněnost případného vyloučení) bezpečnostních opatření;
- Předmětem stanovení pravidel a postupů musí být:
  - řízení rizik;
  - řízení přístupů k informačním systémům a aplikacím;
  - bezpečné chování uživatelů;
  - bezpečnostní vzdělávání;
  - řízení dodavatelů HW, SW a služeb;
  - pravidla pro pseudonymizaci a šifrování dat;
  - řízení technických zranitelností;
  - řízení kontinuity činností;
  - zálohování;
  - monitorování, kontrola a vyhodnocování účinnosti opatření.
- Stanovit odpovědnost a kompetence za i při realizaci stanovených pravidel.

5.16 NÁVRH PROCESŮ K ZAJIŠTĚNÍ PRAVIDELNÉHO TESTOVÁNÍ A VYHODNOCOVÁNÍ ÚČINNOSTI PŘIJATÝCH TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ

- přezkoumání účinnosti technických a organizačních opatření
- aktualizovat Plán kontrol a hospitační činnosti MGO

6. ANALÝZA A ŘÍZENÍ RIZIK

Rizika byla hodnocena v souladu s metodikou hodnocení rizik dle přílohy č. 2 Hodnocení rizik vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Jednotlivá rizika byla vyhodnocena a navrženy postupy k jich eliminaci či snížení dopadu.

6.1 ANALÝZA RIZIK – METODICKÁ VÝCHODISKA

Zpracování osobních údajů bylo, je a po celou dobu uchovávání údajů bude provázeno riziky, jejichž míru působení lze minimalizovat jejich definováním, soustavným vyhodnocováním a případným koncepčním nebo operativním zásahem reagujícím na skutečný výskyt rizika nebo možnost jeho vzniku.

Rizika jsou konkrétní hrozby, které mohou ohrozit subjekt údajů i zpracovatele osobních údajů zejména v případě neoprávněného nakládání s údaji či jejich zničení.

Analýza rizik je pak standardním nástrojem pro řízení a eliminaci rizik v době zpracování a uchovávání osobních údajů. Nová rizika se však mohou objevit i později, především v souvislosti s nově užívanými scénáři zpracování, ať už vycházejí z vlastních potřeb zpracovatele či vznikají v důsledku uplatňování nových legislativních požadavků.

Cílem řízení rizik je podchytit rizika zpracování a uchovávání osobních údajů, vyhodnotit pravděpodobnost jejich vzniku a závažnost dopadů, naplánovat akce směřující ke snížení pravděpodobnosti vzniku rizikové události a akce směřující ke zmírnění negativních dopadů rizikové události, pokud už nastane.

V některých případech je možné, na identifikované riziko, vědomě reagovat rozhodnutím o akceptaci rizika bez nějakých protiopatření, neboť ta jsou buď nemožná nebo příliš časově či finančně nákladná. Všechny aktivity zahrnuté ve zpracování a uchovávání osobních údajů svým charakterem naplňují požadavky kladené na definici rizik. Zpracování osobních údajů probíhá v rizikovém prostředí, s nímž jsou spojené výdaje na zabezpečení údajů. Prvním krokem procesu snižování rizik je proto jejich analýza. Analýza rizik pro potřeby ochrany osobních údajů je chápána jako proces definování hrozeb, pravděpodobnosti jejich výskytu a dopadu na aktivity, tedy stanovení rizika jejich závažnosti.

Analýza zahrnuje následující kroky:

- 1. rozbor vzájemných vztahů, kontextu a souvislostí procesů spojených se zpracování a uchováváním osobních údajů,
- 2. vytvoření základního souboru potenciálních rizik v procesech, operacích a činnostech v souladu s legislativními normami, případně dalšími normami a dokumenty ČR a EU,
- 3. výběr souboru rizik, která jsou důležitá z hlediska ochrany osobních údajů,
- 4. sestavení pořadí rizik podle určeného stupně významnosti pro stanovení priorit rizik,

- 5. zpracování návrhu řešení eliminace nebo zmírnění rizik v průběhu zpracování a uchovávání osobních údajů.

6.2 KLASIFIKACE RIZIK A JEJICH DOPADŮ

Jedním z významných aspektů řízení rizik je identifikace (definice) potenciálních rizik, která lze na úrovni zpracování a uchovávání osobních údajů dle svého charakteru rozdělit do předem definovaných klasifikačních skupin:

A. rizika personální (zaměstnanecká)

B. rizika realizace smluv

C. rizika technická

D. rizika provozní

E. rizika vyšší moci

F. rizika realizace jednotlivých scénářů

Následující tabulky představují výsledný seznam identifikovaných potenciálních rizik. Pro zvýšení přehlednosti byla jednotlivá rizika označena kódem (např. A.1, B.3, apod.).

Tabulka číslo 4 **Tabulky rizik**

A Rizika personální	
kód	rizika
A.1	Sběr OÚ provádí neoprávněná osoba
A.2	Osoba oprávněná k nakládání s OÚ není zavázána k mlčenlivosti
A.3	Neoprávněný přístup do IS a aplikací
A.4	Neoprávněný přístup k fyzicky uloženým dokumentům
B Rizika realizace smluv	
kód	rizika
B.1	Smlouva neobsahuje ustanovení o ochraně OÚ
B.2	Smlouva obsahuje ustanovení o ochraně OÚ pouze v obecné podobě
B.3	Smluvní partner neoprávněně nakládá s OÚ
B.4	Smlouvy zpřístupňované veřejnosti nejsou anonymizovány
C Rizika realizace jednotlivých scénářů	
kód	rizika
C.1	Náhodné nebo protiprávní zničení údajů
C.2	Ztráta údajů
C.3	Pozměňování údajů

C.4	Neoprávněné zpřístupnění předávaných údajů
C.5	Neoprávněné zpřístupnění uložených údajů
C.6	Neoprávněné zpřístupnění jinak zpracovávaných údajů
C.7	Neoprávněný přístup k údajům
D Rizika provozní	
kód	rizika
D.1	Příliš široké popsání scénáře zpracování
D.2	Nevhodně nastavená doba uchovávání
D.3	Nedostatečné vymezení ochrany OÚ v pracovní smlouvě, DPČ či DPP
D.4	Nedostatečné zabezpečení dokumentů uložených ve fyzické podobě
D.5	Nedostatečné zabezpečení nakládání s OÚ v interních směrnicích
D.6	Subjekty údajů nejsou informovány o svých právech
D.7	Není vyžadován povinný souhlas se zpracováním OÚ
E Rizika vyšší moci	
kód	rizika
E.1	Živelná pohroma
E.2	Krádež technologií nebo jejich poničení
E.3	Teroristický útok
E.4	Kybernetický útok

6.3 HODNOCENÍ RIZIK

Druhou fází analýzy rizik je jejich vyhodnocení, které spočívá v určení **míry dopadu „D"** rizika, **hrozby „H"** a **zranitelnosti „Z"**

Míra dopadu, hrozby a zranitelnosti je hodnocena metodikou dle přílohy č. 2 Hodnocení rizik vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Jednotlivé úrovně hodnocení byly vyjádřeny číselně od 1 (nízká úroveň) do 4 (kritická úroveň). Jako funkce komplexního hodnocení rizika byla zvolena funkce

$$\textbf{úroveň rizika} = D^2 + H^2 + Z^2$$

Jestliže si dopad, hrozbu a zranitelnost představíme jako osy popisující třírozměrný prostor, pak zvolená funkce reflektuje „vzdálenost" daného rizika od nejnižší možné kombinace dopadu, hrozby a zranitelnosti, tj. D = H = Z = 1.

S ohledem na rozložení možností hodnocení dopadu, hrozby a zranitelnosti bylo celkové riziko vymezeno jako

nízké úroveň rizika se pohybuje od 3 do 14

střední úroveň rizika se pohybuje od 15 do 22

vysoké úroveň rizika se pohybuje od 23 do 29

kritické úroveň rizika se pohybuje od 30 do 48

Tabulky hodnocení dopadů, hrozeb, zranitelnosti a úrovně rizika

Stupnice pro hodnocení dopadů D	
Úroveň	**Popis**
Nízká 1	Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický. Rozsah případných škod nepřesahuje a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty do 5000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob.
Střední 2	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí a) do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 5000000 Kč do 50000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2500 osob.
Vysoká 3	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí a) od 11 do 100 mrtvých nebo od 101 do 1000 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 50000000 Kč do 500000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2501 do 25000 osob.
Kritická 4	Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí a) 101 a více mrtvých a 1001 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty převyšující 500000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25000 osob.
Stupnice pro hodnocení hrozeb H	
Úroveň	**Popis**
Nízká 1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední 2	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká 3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická 4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stupnice pro hodnocení zranitelností Z	
Úroveň	**Popis**
Nízká 1	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední 2	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká 3	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická 4	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.
Stupnice pro hodnocení rizik	
Úroveň	**Popis**
Nízká 3-14	Riziko je považováno za přijatelné.
Střední 15-22	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoká 23-29	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická 30-48	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Cílem této podkapitoly tedy bylo vytvoření tzv. **katalogu rizik**, ve kterém jsou uvedeny hodnoty pro míru hrozby, dopadu, zranitelnosti a hodnocení rizik. Následující tabulka představuje výsledný katalog rizik – souhrn potenciálních rizik, která mohou nastat v procesu nakládání s osobními údaji. Tabulky k jednotlivým scénářům jsou uvedeny přímo u popisu scénářů. Důvodem pro toto řešení je skutečnost, že rizika personální, rizika realizace smluv, rizika provozní a rizika vyšší moci se dotýkají celé organizace bez ohledu na realizovaný scénář zpracování osobních údajů.

Katalog rizik

A Rizika personální					
kód	rizika	D	H	Z	riziko
A.1	Sběr OÚ provádí neoprávněná osoba	2	1	3	14, nízké
A.2	Osoba oprávněná k nakládání s OÚ není zavázána k mlčenlivosti	2	1	3	14, nízké
A.3	Neoprávněný	2	3	3	22,

	přístup do IS a aplikací				střední
A.4	Neoprávněný přístup k fyzicky uloženým dokumentům	2	2	3	17, střední
B Rizika realizace smluv					
kód	rizika	D	H	Z	riziko
B.1	Smlouva neobsahuje ustanovení o ochraně OÚ	3	2	4	29, vysoké
B.2	Smlouva obsahuje ustanovení o ochraně OÚ pouze v obecné podobě	2	4	3	29, vysoké
B.3	Smluvní partner neoprávněně nakládá s OÚ	4	2	4	36, kritické
B.4	Smlouvy zpřístupňované veřejnosti nejsou anonymizovány	3	2	4	29, vysoké
D Rizika provozní					
kód	rizika	D	H	Z	riziko
D.1	Příliš široké popsání scénáře zpracování	2	2	3	17, střední
D.2	Nevhodně nastavená doba uchovávání	2	4	3	29, vysoké
D.3	Nedostatečné vymezení ochrany OÚ v pracovní smlouvě, DPČ či DPP	1	4	3	26, vysoké
D.4	Nedostatečné zabezpečení dokumentů uložených ve fyzické podobě	2	2	4	24, vysoké
D.5	Nedostatečné zabezpečení nakládání s OÚ v interních směrnicích	3	3	3	27, vysoké
D.6	Subjekty údajů nejsou	2	3	3	22, střední

	informovány o svých právech				
D.7	Není vyžadován povinný souhlas se zpracováním OÚ	2	2	3	17, střední
E Rizika vyšší moci					
kód	rizika	D	H	Z	riziko
E.1	Živelná pohroma	4	1	2	21, střední
E.2	Krádež technologií nebo jejich poničení	4	1	2	21, střední
E.3	Teroristický útok	4	1	2	21, střední
E.4	Kybernetický útok	4	1	2	21, střední

6.4 ELIMINACE RIZIK

Na analýzu rizik navazují opatření, jejichž cílem je úplná eliminace potenciálních rizik nebo alespoň jejich minimalizace do podoby, která již projekt zásadně neovlivní a neohrozí jeho průběh.

Taktika řízení rizik spočívá ve výběru nejvhodnějšího postupu pro zvládání příslušného rizika. Zvládání rizika spočívá obecně ve snižování jeho dopadu anebo pravděpodobnosti jeho výskytu. Pro kritická rizika se stanovují tzv. generické taktiky k jejich zvládnutí výběrem jedné z dále uvedených metod:

- **vyloučení rizika** – zákaz vybraných rizikových aktivit a procesů;
- **snížení rizika** – snížení velikosti dopadu např. pojištěním rizika;
- **přenos rizika** – redukce rizika snížením pravděpodobnosti nežádoucích událostí;
- **přijetí rizika** – akceptace rizika na stávající úrovni bez dalších aktivit;

Volba základní taktiky vychází z disponibilních možností, jakými vůbec lze v principu snížit dopad a pravděpodobnost konkrétního rizika.

Smyslem základních taktik je především uvědomění si základního směru (resp. možnosti) pro snižování významností rizika (tj. směru zamýšleného posunu pozice rizika v mapě rizik, a to prostřednictvím snižování jeho pravděpodobnosti anebo dopadu s cílem posunout „pozici" rizika v mapě rizik co nejvíce k počátku).

Pro eliminaci identifikovaných rizik byla vždy zvolena vhodná taktika zvládání rizika, která vedla ke stanovení konkrétního opatření. Opatření pro rizika realizace jednotlivých scénářů jsou obsažena v doporučeních pro konkrétní scénář.

Opatření navržená pro eliminaci rizik

A Rizika personální		
kód	rizika	opatření vedoucí k eliminaci
A.1	Sběr OÚ provádí neoprávněná osoba	Jasné vymezení pracovních povinností zaměstnanců
A.2	Osoba oprávněná k nakládání s OÚ není zavázána k mlčenlivosti	Příslušné ustanovení pracovní smlouvy; v případě osob, které nejsou zaměstnanci organizace zajistit vhodným smluvním nástrojem
A.3	Neoprávněný přístup do IS a aplikací	Důsledné dodržování bezpečnostních opatření při používání IT prostředků, opakované seznamování pracovníků s principy IT bezpečnosti
A.4	Neoprávněný přístup k fyzicky uloženým dokumentům	Pravidelná kontrola fyzického zabezpečení a evidence oprávněných osob
B Rizika realizace smluv		
kód	rizika	opatření vedoucí k eliminaci
B.1	Smlouva neobsahuje ustanovení o ochraně OÚ	Zapracovat ustanovení o ochraně OÚ do návrhů smluv
B.2	Smlouva obsahuje ustanovení o ochraně OÚ pouze v obecné podobě	Konkretizovat ve smlouvách nakládání s OÚ
B.3	Smluvní partner neoprávněně nakládá s OÚ	Stanovit ve smlouvách dostatečné sankční podmínky a v případě porušení ochrany OÚ vyžadovat plnění sankcí
B.4	Smlouvy zpřístupňované veřejnosti nejsou anonymizovány	Stanovit osobní zodpovědnost zaměstnance za zveřejňování smluv (včetně publikace materiálů pro jednání zastupitelstva) s příslušnými sankcemi za porušení povinností
D Rizika provozní		
kód	rizika	opatření vedoucí k eliminaci
D.1	Příliš široké popsání scénáře zpracování	Rozdělit některé scénáře zpracování OÚ do meších více konzistentních celků
D.2	Nevhodně nastavená doba uchovávání	1. Ověřit zákonné opodstatnění pro dobu uchovávání OÚ (opodstatnění musí vycházet z odvětvového zákona, nikoli ze zákona č. 499/2004 Sb., o archivnictví a spisové službě) 2. Zrevidovat spisový a skartační řád KÚ tak, aby doby uschovávání odpovídaly zákonným požadavkům

D.3	Nedostatečné vymezení ochrany OÚ v pracovní smlouvě, DPČ či DPP	Upravit pracovní smlouvy (např. dodatkem) tak, aby každý zaměstnanec měl jasně vymezeno, s jakým typem OÚ a jakým způsobem může nakládat; stanovit postihy za případné porušení povinností
D.4	Nedostatečné zabezpečení dokumentů uložených ve fyzické podobě	1. Revidovat interní směrnice týkajících se zabezpečení dokumentů 2. pravidelně kontrolovat dodržování interních směrnic 3. pravidelně kontrolovat fyzické zabezpečení dokumentů
D.5	Nedostatečné zabezpečení nakládání s OÚ v interních směrnicích	Revidovat interní směrnice tak, aby bylo nakládání s OÚ podrobně popsáno, pokud možno včetně zákonného odůvodnění zvoleného postupu
D.6	Subjekty údajů nejsou informovány o svých právech	Systematicky informovat subjekty údajů o právech garantovaných GDPR
D.7	Není vyžadován povinný souhlas se zpracováním OÚ	Systematicky vyžadovat povinný souhlas subjektu údajů se zpracovnám OÚ
E Rizika vyšší moci		
kód	rizika	opatření vedoucí k eliminaci
E.1	Živelná pohroma	Důsledně uplatňovat prvky krizového řízení
E.2	Krádež technologií nebo jejich poničení	Důsledně uplatňovat prvky krizového řízení včetně zálohování dat c různých lokalitách
E.3	Teroristický útok	Důsledně uplatňovat prvky krizového řízení
E.4	Kybernetický útok	Důsledně uplatňovat prvky krizového řízení

7. ZÁVĚR A DOPORUČENÍ K DALŠÍMU POSTUPU

Jedním ze základních znaků ochrany osobních údajů podle GDPR je kontinuita, kterou lze chápat tak, že pokud správce splňuje požadavky podle stávajícího zákona o ochraně osobních údajů, z velké části splňuje také požadavky GDPR. Jen v jednotlivostech je nutné zavedený systém ochrany osobních údajů vhodně přizpůsobit úpravou stávajících a zavedením nových procesů či opatření.

Analýzou stávajícího stavu zpracování a ochrany osobních údajů na Matičním gymnáziu Ostrava byly pojmenovány účely a rozsah zpracování osobních údajů, čímž byly verifikovány výchozí informace k posouzení shody či neshody s požadavky jak stávajícího zákona o ochraně osobních údajů a řadou zvláštních souvisejících zákonů, tak i s legislativou ochrany osobních údajů, tedy s Obecným nařízením GDPR.

Provedením analýzy byly zjištěny dílčí neshody, které jsou konkrétně uvedeny v jednotlivých částech textu analýzy a vždy s návrhem řešení uvedeným jako doporučení, poznámka nebo možné způsoby či varianty řešení. Pozitivem je, že se nejedná o zásadní skutečnosti ohrožující bezpečnost osobních údajů.

7.1 NUTNÉ KROKY DALŠÍHO POSTUPU

Konkrétní činnosti a předpokládané využití tohoto analytického dokumentu pro dosažení souladu s GDPR:

- jmenovat pověřence pro ochranu osobních údajů a stanovit jeho povinnosti a odpovědnosti (v kompetenci zřizovatel do 18. 5. 2018);
- současně s odpovědnými zaměstnanci:
    - realizovat doporučení ke zpracování osobních údajů, která jsou uvedena u příslušných účelů zpracování (scénářů);
    - posoudit a rozhodnout o navrhovaných řešeních či variantách, která jsou uvedena v příslušných pasážích dokumentu, tato následně realizovat v praxi;
    - aktualizovat smlouvy se společnostmi identifikovanými v analýze v pozici zpracovatele nebo subzpracovatele, doplnit je o příslušná ustanovení z hlediska ochrany osobních údajů (např. formou dodatků nebo uzavřít zpracovatelské smlouvy). Obdobně prověřit a aktualizovat smlouvy s dalšími osobami, které se mohou v rámci plnění předmětu smlouvy seznámit s osobními údaji.
- při implementaci GDPR je nutné průběžně sledovat zveřejňované informace ke GDPR, zejména webové stránky Úřadu pro ochranu osobních údajů, kde je této problematice věnována samostatná sekce. Na těchto stránkách jsou a také budou průběžně zveřejňována „vodítka pracovní skupiny WP29", což jsou metodické výklady k některým, zejména novým, ustanovením GDPR.
- Proces implementace ukončit proškolením vybraných zaměstnanců k upraveným či novým procesům a opatřením při zpracování a ochraně osobních údajů.
- Toto školení by měl vést pověřenec pro ochranu osobních údajů, jelikož obsah školení by měl být zaměřen do konkrétních oblastí a zohledňovat specifika SŠ.

- Prověřit právní opodstatnění pro dobu uchovávání OÚ ve scénářích, kde je uvedeno doporučení k takovému prověření. Doba uchovávání přitom musí vycházet z příslušných odvětvových zákonů, nikoli obecně ze zákona č. 499/2000 Sb., o archivnictví a spisové službě.
- Upravit spisový a skartační řád v návaznosti na zjištění podle předchozího bodu.

Zahájení rutinního provozu se předpokládá nejpozději dnem nabytí účinnosti GDPR, tj. 25. května 2018. Významným úkolem pověřence bude průběžný monitoring informací ke GDPR, a to zejména judikáty různých soudních dvorů států Evropské unie k problémům, které vyvstaly z realizace požadavků GDPR napříč členskými státy Evropské unie.

7.2 INFORMACE ZVEŘEJNĚNÉ NA WEBOVÝCH STRÁNKÁCH MGO

Cílem analýzy bylo zjistit, zda jsou na webových stránkách SŠ zveřejňovány informace týkající se ochrany osobních údajů a jaká je úroveň těchto informací.

GDPR přímo neuvádí požadavky na zveřejňované informace, ale v rámci principu férovosti a transparentnosti se předpokládá řádné informování o stavu zpracování a ochrany osobních údajů zpracovávaných SŠ. Informování o zajištění ochrany osobních údajů je také vhodnou propagací péče společnosti o tyto údaje.

V současné době je obsah informací z hlediska ochrany osobních údajů na frontpage webu SŠ nedostupný. Zřízení webové sekce Ochrana OÚ a vytvoření dokumentace pro webovou sekci j podmíněno dodáním patřičné dokumentace zřizovatelem do 30. 4. 2018, respektiv do 11. 5. 2018.

Je zcela nezbytné upravit zveřejněné informace tak, aby byly v souladu s právní úpravou současnou a následně požadavky GDPR a to zejména na základě upřesnění právních základů pro jednotlivá zpracování osobních údajů.

Cookies nejsou v rámci webu vůbec používány a uživatel nedává souhlas s jejich využitím.

Frontpage webu bude informovat o kontaktu na Pověřence pro ochranu osobních údajů s uvedením telefonu a emailu.

7.3 POSOUZENÍ STAVU STÁVAJÍCÍCH INTERNÍCH SYSTÉMŮ

Cílem posouzení bylo zjistit, jaký je aktuální stav místně spravovaných interních systémů na Matičním gymnáziu Ostrava ve vztahu k technologickým a procesním požadavkům, které na bezpečnost zpracování klade článek 32 GDPR.

Obecně nařízení GDPR požaduje, aby správce i zpracovatel zajistili takovou úroveň zabezpečení, jež bude odpovídat zjištěným rizikům, která představuje zpracování, náhodné či úmyslné zničení, ztráta, pozměňování nebo neoprávněný přístup k datům. Prakticky se jedná zejména o následující opatření:

- pseudonymizace a šifrování osobních dat;

- schopnost zajistit důvěrnost, integritu, dostupnost a odolnost systémů a služeb pro zpracování osobních údajů;
- schopnost obnovit dostupnost osobních údajů a přístupu k nim v případě technických incidentů;
- existence procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření;

Dostupnost je zajištěna díky zálohování a možnosti automatického přechodu na záložní systémy ve druhé lokalitě technologického centra.

7.4 STÁVAJÍCÍ PODMÍNKY PRO ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Cílem posouzení bylo zmapovat a popsat stávající podmínky a proces pro řízení bezpečnostních incidentů s důrazem na možnosti pokrytí požadavků nařízení GDPR na procesy ohlašování a oznamování případů porušení zabezpečení osobních údajů dozorovému úřadu a subjektům údajů – články 32 a 33 GDPR.

MGO je povinno pokud možno do 72 hodin ohlásit dozorovému úřadu jakékoliv porušení zabezpečení osobních údajů, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Dané ohlášení pak musí obsahovat minimálně následující:

- popis povahy daného porušení, kategorii a přibližný počet dotčených subjektů, kategorii a druh dotčených záznamů;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů v organizaci případně jiné kontaktní místo, které může v případě potřeby poskytnout další informace;
- popis pravděpodobných důsledků porušení zabezpečení;
- popis opatření, která správce navrhl k přijetí s cílem vyřešit dané porušení zabezpečení včetně opatření pro zmírnění případných nepříznivých dopadů.

Správce veškeré identifikované porušení zabezpečení osobních údajů dokumentuje tak, že uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

V případě, že je pravděpodobné, že určitý případ porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob, je správce povinen toto oznámit bez zbytečného odkladu subjektu údajů. Toto oznámení může být v případě, že by vyžadovalo nepřiměřeně vysoké úsilí, provedeno pomocí veřejného oznámení nebo podobného opatření.

V organizaci SŠ je zaveden zdokumentovaný definovaný proces řízení bezpečnostních incidentů z hlediska GDPR. Proces řízení incidentů provozních a technických je popsán v Pravidlech pro zvládání bezpečnostních událostí a incidentů.

V systému je udržována veškerá historie týkající se již vyřešených a uzavřených incidentů.

8. PŘÍLOHA – DOPORUČENÍ KE KAMEROVÉMU SYSTÉMU

Fotografie a video záznamy osob jsou z hlediska GDPR chápány jako osobní údaje, stejně jako informace o osobách, které jsou odvozeny z těchto materiálů - například registrační čísla vozidel. Většina užití kamerových systémů organizacemi nebo firmami je upravena zákonem, bez ohledu na počet kamer nebo na složitost zařízení.

Dosud každý kdo chtěl, tak v zásadě mohl instalovat kamerový systém, aniž by nějak zvlášť musel přemýšlet o důsledcích takového konání. Nařízení GDPR chápe použití kamerových systémů, jako sběr osobních dat, pokud na záznamech lze rozpoznat tváře jednotlivých osob. V současné době je kvalita kamer do té míry vysoká, že se to týká prakticky jakéhokoliv provozovatele CCTV systému. Instalací kamer se dotyčná organizace stává správcem osobních údajů a s tím přichází patřičná odpovědnost. Správce musí být v první řadě schopen odůvodnit získávání a zpracovávání osobních údajů prostřednictvím CCTV systému.

Pokud se organizace rozhodne k instalaci kamer okolo svého objektu kvůli zajištění bezpečnosti, pak by takové jednání mělo být snadno ospravedlnitelné. Pokud organizace dokáže instalaci kamer obhájit jako nezbytnost z hlediska bezpečnosti a ochrany zdraví, zejména vzhledem k předchozím událostem, pak to může být přijatelné.

Při snímkování, kde lze očekávat soukromí, musíte potřebu snímání dostatečně ospravedlnit. Například snaha instalovat kamerový systém v klidné ulici rodinných domů, kde v minulosti nedošlo k žádnému incidentu, je obtížně ospravedlnitelná. Naopak bez problémů lze aktivovat kamerový systém v centru města u rušného nádraží.

K povinnostem provozovatele kamerového systému patří sdělit osobám, které mohou být snímány, že k takové činnosti dochází a kdo za systém zodpovídá. Účel shromažďovaných údajů by měl být jasný a zřejmý. Pokud se jedná o monitorování zaměstnanců nebo o zdraví a bezpečnost, je nezbytné tuto skutečnost všem osobám zachycených na záběrech kamer, jasně a srozumitelně komunikovat. Označení v místě snímání například piktogramem s kontaktem na provozovatele je dostatečné.

Správce dat musí poskytnout dostatečné argumenty pro ukládání a uchovávání dat. Rozumná doba pro uchování záběrů z kamer činí maximálně 30 dní. Pokud se organizace rozhodne pro delší periodu, pak samozřejmě může, ale musí toto rozhodnutí podpořit analýzou rizik pro subjekty údajů a dostatečně odůvodnit orgánu dohledu. Moderní kamerové systémy umožňují již ve svém základu nastavit retenční limity pro jednotlivé kamery.

GDPR jasně hovoří o tom, že povinností každého správce osobních údajů je na žádost subjektu údajů poskytnout k dispozici veškerá data, která o něm správce uchovává v běžně dostupném formátu. Toto ustanovení se netýká jen textových údajů v databázích, ale samozřejmě také obrazových záznamů. V zásadě každá osoba, jejíž obraz je zaznamenáván na kamerovém systému, má právo požádat a získat kopie vlastních osobních údajů ze záznamu. K uplatnění tohoto práva musí dotyčná osoba podat písemnou žádost. Správce údajů může za odpověď na tuto žádost účtovat přiměřený poplatek a musí odpovědět do jednoho měsíce. Takže každý, kdo je zachycen CCTV kamerami, má právo požadovat tuto nahrávku, protože se jedná o osobní údaj. Jsou-li na záznamu viditelné nějaké jiné osoby, je potřeba přistoupit k úpravě záznamu, tj. rozostřit tváře jiných osob.

Při podávání žádosti o přístup k CCTV záznamu by měl žadatel poskytnout správci údajů přiměřenou informaci o časovém rámci požadovaného záznamu, tj. měl by poskytnout podrobnosti o přibližné době

a konkrétním datu (dnech), ve kterém byl jeho obraz zaznamenán. Například za nedostačující lze považovat žádost, kdy žadatel chce získat všechny záběry, na kterých je zaznamenán. Namísto toho je nezbytné specifikovat, že žádá o kopie všech CCTV záznamů ve vztahu ke své osobě, které byly pořízeny konkrétního dne v rozmezí určitých hodin a v pojmenovaném místě. Za zřejmé se považuje, že pokud záznam již neexistuje ke dni, kdy správce dat obdrží požadavek na zpřístupnění údajů, nemůže žadatel získat kopii záznamu. Žadatelé by si měli být vědomi toho, že CCTV záznamy jsou obvykle odstraňovány během jednoho měsíce od nahrávání.

Pro správce údajů je povinností v odpovědi na žádost o přístup k osobním datům poskytnout kopii osobních údajů žadatele. Obvykle se jedná o kopii záznamu ve formátu videa. Za okolností, kdy technicky nelze záběr zkopírovat do jiného zařízení nebo za jiných výjimečných okolností, je přijatelné poskytnout fotografie jako alternativu k videozáznamu. V případě řešení žádosti zpřístupněním fotografií, je odpovídající dodat jednu fotografii na jednu vteřinu záznamu, ve kterém se objevil obraz žadatele, aby byla dodržena povinnost předat kopii všech osobních údajů, které jsou uchovávány.

Pokud se na CCTV záznamu objevují obrazy jiných osob, než požadovaného subjektu údajů, je na správci údajů, aby zakryl nebo jinak rozmazal či ztmavil snímky těchto ostatních osob předtím, než dodá kopie záběrů nebo fotografií z požadovaného záznamu žadateli. Řešením také může být žádost správce údajů o souhlas ostatních dotčených stran, jejichž obrazy se objevují na videozáznamu, aby mohl vydat požadovanou kopii záznamu obsahující jejich snímky žadateli

Pokud se správce údajů rozhodne použít technologii ke zpracování osobních údajů, kterou je například kamerový systém pro zachycování a zaznamenávání obrazů živých osob, je povinen plnit požadavky týkající se ochrany osobních údajů, které jim nařízení na takové zpracování údajů ukládá. Ve věci žádostí o přístup k CCTV videozáznamu jsou správci údajů povinni plně vyhovět těmto požadavkům. Tvrzení správce údajů o tom, že nemohou reprodukovat kopie záběrů nebo fotografie, které jsou zhotoveny ze záznamu, jsou nepřijatelné výmluvy v souvislosti se zpracováním žádosti o přístup k osobním údajům. Stručně řečeno, pokud správce údajů používá ke zpracování osobních údajů kamerový systém, přebírá i závazek dodržovat všechny související povinnosti týkající se ochrany údajů.

Podle současného platného zákona 101/2000 Sb. o ochraně osobních údajů je mimo jiné povinností správce ohlásit a zaregistrovat existenci provozování takového CCTV systému. Je třeba upozornit na to, že se jedná pouze o případy, kdy může správce údajů identifikovat osoby, jejichž snímky jsou zachyceny.

9. POUŽITÉ TERMÍNY, ZKRATKY A POJMY

Tabulka číslo 5 **Použité zkratky, termíny a pojmy**

Termín	Význam
Dozorový (kontrolní, dohledový) orgán	Jedná se o instituci pověřenou dozorem nad ochranou osobních údajů. V případě České republiky je odpovědným Úřad pro ochranu osobních údajů.
GDPR	(General Data Protection Regulation) je nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů. Bylo přijato a vstoupilo v platnost v dubnu 2016 a jeho účinnost nastává 25. května 2018 na území celé Evropské unie.
ICT	Informační a komunikační technologie
IS	Informační systém
KÚ	Krajský úřad Moravskoslezského kraje
Profilování	Jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.
Pověřenec ochrany osobních údajů	Je pozice v organizaci, kterou nařizuje pro některé správce a zpracovatele osobních údajů nařízení GDPR. K povinnostem a odpovědnostem pověřence patří například poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech a působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování.
DPO	Data Protection Officer – anglický termín pro Pověřence na ochranu osobních údajů
Posouzení vlivu na ochranu osobních údajů	Nástroj pro řízení rizik, který lze pojmout jako důvodovou zprávu, která obsahuje detailně popsaný záměr včetně všech argumentů a doložení důvodnosti zamýšleného zpracování. Rovněž musí posoudit rizika, která mohou ovlivnit práva a svobody osob, jejichž osobní data budou zpracovávána, a opatření, které správce osobních údajů přijme pro zajištění bezpečnosti opatření.
Správce	Subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.
SŠ	Mendelova střední škola Nový Jičín, příspěvková organizace
ÚOOÚ	Úřad pro ochranu osobních údajů

Zpracovatel	Každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují.
Zákon o ochraně osobních údajů	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
Zpracování osobních údajů	Jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.
Scénář zpracování	Firemní proces, ve kterém dochází k operaci s osobními údaji. Obvykle popisuje postup činnosti spojené se zpracováním osobních údajů.