



General
Data
Protection
Regulation

Nařízení o ochraně osobních údajů

Směrnice GDPR pro příspěvkovou organizaci



Mateřská škola, Náchod,
Vítkova 304
IČ: 70996458

GDPR

Obsah

A. Účel	4
B. Pro koho je určena	4
C. Vysvětlivky odborných pojmů.....	4
D. Stanovení zásad (podle článku 5 nařízení GDPR a zákona č. 110/2019)	5
<i>Zákonnosti.....</i>	<i>5</i>
<i>Podmínky pro udělení souhlasu (podle článku 7 nařízení GDPR a zákona č. 110/2019).....</i>	<i>6</i>
<i>Podmínky použitelné pro souhlas dítěte v souvislosti se službami informační organizace (podle článku 8 nařízení GDPR a zákona č. 110/2019).....</i>	<i>6</i>
<i>Korektnost a transparentnost.....</i>	<i>6</i>
<i>Účelové omezení</i>	<i>7</i>
<i>Minimalizace údajů.....</i>	<i>7</i>
<i>Přesnost</i>	<i>7</i>
<i>Omezení uložení</i>	<i>8</i>
<i>Integrita a důvěrnost.....</i>	<i>8</i>
<i>Odpovědnost</i>	<i>8</i>
E. Zpracování osobních údajů	8
F. Způsoby ochrany osobních údajů	9
<i>Písemná podoba – dokumenty obsahující osobní údaje – v produkčním prostředí.....</i>	<i>9</i>
<i>Písemná podoba – dokumenty obsahující osobní údaje – spisovna (archiv)</i>	<i>9</i>
<i>Elektronická podoba – data obsahující osobní data – produkční databáze a soubory.....</i>	<i>10</i>
<i>Elektronická podoba – data obsahující osobní data – archivní databáze a soubory.....</i>	<i>11</i>
G. Způsoby anonymizace po ukončení doby zpracování osobních údajů	11
H. Způsoby pseudonymizace osobních údajů	12
I. Způsoby předávání osobních údajů v rámci organizace.....	12
J. Způsoby předávání osobních údajů jiným zpracovatelům	12
K. Způsoby předávání osobních údajů dalším příjemcům	12
L. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (podle článku 44 nařízení GDPR a zákona č. 110/2019)	13
M. Zpracování osobních údajů za účelem cíleného marketingu.....	13
N. Práva fyzických osob (podle nařízení GDPR a zákona č. 110/2019).....	13
<i>Právo subjektu údajů na přístup k osobním údajům (podle článku 15 nařízení GDPR a zákona č. 110/2019).....</i>	<i>14</i>
<i>Zajištění práva přenositelnosti subjektu údajů (podle článku 20 nařízení GDPR a zákona č. 110/2019).....</i>	<i>15</i>
<i>Právo fyzické osoby na opravu (podle článku 16 nařízení GDPR a zákona č. 110/2019).....</i>	<i>15</i>
<i>Právo fyzické osoby na výmaz (podle článku 17 nařízení GDPR a zákona č. 110/2019)</i>	<i>16</i>
<i>Právo na omezení zpracování (podle článku 18 nařízení GDPR a zákona č. 110/2019).....</i>	<i>16</i>

O. Hlášení bezpečnostních incidentů <i>(podle článku 33 nařízení GDPR a zákona č. 110/2019)</i>	16
P. Stanovení Pověřence pro ochranu osobních údajů (DPO) <i>(podle článku 37 nařízení GDPR a zákona č. 110/2019)</i>	17
Q. Školení pracovníků, kteří přicházejí do styku s osobními údaji.....	18
R. Oddělení v organizaci, která se řídí směrnicí.....	19
Udělení souhlasu s poskytnutím osobních údajů	20
Zrušení uděleného souhlasu k poskytnutí osobních údajů	21
Příloha č. 1: Udělení souhlasu s poskytnutím osobních údajů	22
Příloha č. 2: Zrušení uděleného souhlasu k poskytnutí osobních údajů.....	23
Příloha č. 3: Karta evidovaných osobních údajů v organizaci o subjektu údajů/ fyzické osobě	24
Příloha č. 4: Varianta zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem	25
Příloha č. 5: Varianta zabezpečení odesílaných příloh elektro. poštou – doplnění souboru heslem – PDF	27
Příloha č. 6: Vzor ohlášení dozorovému úřadu	30
Záznam o činnostech zpracování – informační systémy – vzor	31
Záznam o činnostech zpracování – dokumenty – vzor	33
Záznam o činnostech zpracování – informační systémy – Správa MŠ.....	35
Záznam o činnostech zpracování – informační systémy – VIS Plzeň	37
Záznam o činnostech zpracování – informační systémy – Mozilla Thunderbird.....	39
Záznam o činnostech zpracování - dokumenty – Mzdová a personální agenda	41
Záznam o činnostech zpracování - dokumenty – Evidence dětí.....	44
Záznam o činnostech zpracování - dokumenty – Stravování.....	46
Záznam o činnostech zpracování - dokumenty - Účetnictví.....	48
Záznam o činnostech zpracování - dokumenty – Kniha pošty	50
Záznam o činnostech zpracování – informační systémy – Kamerový systém.....	52
S. Prezenční listina pracovníků, kteří jsou seznámeni se směrnicí k GDPR a zákonu č. 110/2019	54



A. Účel

Účelem této směrnice je stanovení základních zásad a pravidel pro ochranu a zpracování osobních údajů fyzických osob v organizaci, a to jak v listinné, tak i elektronické podobě. Jednotlivá pravidla jsou stanovena pro všechny pracovníky, kteří přicházejí do styku s osobními údaji fyzických osob.

Fyzická osoba je osoba, kterou lze přímo nebo nepřímo identifikovat zejména odkazem na určitý identifikátor, například jméno, osobní číslo, bydliště nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychologické, ekonomické, kulturní či společenské identity této fyzické osoby.

Tato směrnice se řídí **platnými právními předpisy**, zejména:

- ➔ nařízením Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (GDPR),
- ➔ zákonem č. 110/2019 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

B. Pro koho je určena

Pro všechny pracovníky organizace, kteří přicházejí do styku s osobními údaji subjektu údajů (fyzických osob).

C. Vysvětlivky odborných pojmů

V tomto oddíle jsou popsány vysvětlivky některých pojmů, které jsou ve směrnici použity.

Osobní údaj – jakákoli informace, která vede k identifikaci fyzické osoby (například jméno, příjmení, bydliště, telefon, email atd.)

Citlivý osobní údaj – jedná se o jakýkoli osobní údaj, který může mít v případě jeho zneužití, zcizení či předání neoprávněným osobám, větší negativní újmu na fyzickou osobu (například zdravotní dokumentace, finanční situace apod.)

Zvláštní osobní údaj – jedná se o osobní údaj, který může správce zpracovávat jen na základě informovaného souhlasu podle nařízení

Anonymní osobní údaj – jedná se o údaj, který nemůže ani spojením s jinou informací vést k identifikaci fyzické osoby

Odpovědná osoba – jedná se o každého pracovníka organizace, který je oprávněn ke zpracování osobních údajů, a který je i řádně proškolen k těmto činnostem (například finanční účetní, mzdová účetní, ředitel organizace atd.)

Anonymizace osobních údajů – jedná se o operaci v podobě úpravy osobních údajů do takové podoby, která nadále neumožňuje určit konkrétní fyzickou osobu (například skartace, výmaz souboru, výmaz údajů z databáze atd.)

Subjekt údajů – fyzická osoba, která je předmětem ochrany osobních údajů (například pracovník, zákazník, dodavatel, student)

Nařízení - nařízení 2016/679 Evropského parlamentu a Rady (EU).

Správce – organizace, která provádí zpracování osobních údajů fyzických osob (subjektu údajů), vlastník směrnice GDPR.

Zpracovatel – organizace, která provádí zpracování osobních údajů pro správce. Zpracovatel vždy zpracovává osobní údaje pouze dle pokynů správce a je za jejich ochranu odpovědný správci. Mezi správcem a zpracovatelem je vždy uzavřena smlouva o zpracování osobních údajů.

Příjemce – každá organizace, která přijímá osobní údaje fyzických osob od správce, ale nadále je správcí nevrací k jeho dalšímu zpracování (úřady apod.)

Pověřenec pro ochranu osobních údajů – pracovní pozice, smluvní fyzická nebo právnická osoba, která vykonává pro správce činnost k zabezpečení ochrany při zpracování osobních údajů. Některé organizace mají podle nařízení mít pověřence (státní instituce, organizace, které zpracovávají).

Zpracování – rozumí se jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů jako je shromáždění, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

D. Stanovení zásad *(podle článku 5 nařízení GDPR a zákona č. 110/2019)*

Organizace se řídí jednotlivými zásadami, které stanovuje nařízení GDPR a zákon č. 110/2019. Organizace zpracovává osobní údaje v elektronických i listinných dokumentech, souborech či databázích v rámci jednotlivých informačních systémů.

Pracovníci organizace, kteří přicházejí do styku s osobními údaji, respektují pravidla:

Zákonnosti

Každý nový osobní údaj v novém dokumentu (souboru, databázi) je prověřován z hlediska právního nároku, na základě kterého jej organizace má právo zpracovávat.

Organizace má právo ke zpracování osobních údajů na základě:

- ➔ **Právní povinnosti** – zpracování osobních údajů podle příslušného zákona, vyhlášky apod.
- ➔ **Oprávněného zájmu** – zpracování osobních údajů na základě oprávněného zájmu organizace, který však nesmí neúměrně poškozovat ochranu soukromí fyzické osoby
- ➔ **Na základě plnění či uzavření smlouvy** – zpracování osobních údajů na základě uzavřené smlouvy

Ve výjimečných případech zpracovává organizace osobní údaje na základě souhlasu subjektu údajů. Souhlas subjektu údajů je podáván vždy v písemné podobě na schváleném tiskopisu. Vzor tiskopisu schválení se zpracováním osobních údajů je součástí směrnice. Tiskopis obsahuje jméno fyzické osoby, podpis a datum od kdy je dán souhlas. Dále účel k jakému je souhlas udělen. Organizace vede přesnou a zabezpečenou evidenci souhlasů se zpracováním osobních údajů. Jednotlivé souhlasy jsou evidovány po dobu, na kterou byly uděleny. Po zrušení udělení souhlasu jsou údaje, které byly zpracovávány na základě uděleného souhlasu, anonymizovány.

- ➔ Zákonnost zpracování osobních údajů uložených v elektronické podobě (software, soubory) nebo listinné (dokumenty) je popsána v přílohách Záznamy o činnostech používaných v organizaci.
- ➔ Evidence udělených souhlasů obsahuje jméno a příjmení osoby, která udělila souhlas, u dětí i jméno dítěte, za které udělil souhlas jeho zákonný zástupce, datum udělení souhlasu, účel, pro který byl souhlas udělen. V případě, že může v rámci organizace být i více, jak jedna fyzická osoba se stejným jménem a příjmením, potom se v evidenci použije i další rozlišovací údaj (osobní číslo pracovníka, datum narození apod.).

Podmínky pro udělení souhlasu (podle článku 7 nařízení GDPR a zákona č.110/2019)

Organizace pro udělení souhlasu se řídí zejména:

- Pravidlem doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů v elektronické (například e-mailem či potvrzením v databázi dostupné přes webové rozhraní) nebo listinné podobě (vzor souhlasu je součástí směrnice).
- Pokud je souhlas vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, je žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků.
- Subjekt údajů má možnost stejně jednoduchým způsobem svůj souhlas kdykoli odvolat. Odvoláním souhlasu však není dotčena zákonnost zpracování v organizaci po dobu jeho platnosti.
- Organizace nevyžaduje udělení souhlasu formou telefonického rozhovoru.

Podmínky použitelné pro souhlas dítěte v souvislosti se službami informační organizace (podle článku 8 nařízení GDPR a zákona č. 110/2019)

Budou-li v organizaci zpracovávána osobní data dítěte pro jiné, než právním nárokem dané účely (kde je vyžadován souhlas), jsou respektována tato pravidla:

- V případě, že věk osoby je minimálně 15 let, organizace může žádat o souhlas přímo tuto osobu a ne jejího zákonného zástupce. Musí však splnit povinnost, aby obsah souhlasu odpovídal mentální úrovni dané věku fyzické osoby.
- Je-li dítě mladší 15 let, organizace zajistí pro zákonnost takového zpracování osobních údajů souhlas osoby, která vykonává rodičovskou povinnost k dítěti.
- Organizace má zajištěno, aby souhlasy se zpracováním osobních údajů byly formulovány tak, že jim porozumí i osoba s mentálním vývojem odpovídajícím jeho věku.

U každé skupiny osobních údajů je jasně uvedeno, podle jakého právního rámce jsou osobní údaje vedeny.

Korektnost a transparentnost

Organizace zpracovává pouze ty osobní údaje, na které má právní nárok. Zpracování osobních údajů je ze strany organizace korektní a transparentní vůči všem subjektům údajů (fyzickým osobám). Zástupce organizace informuje při získávání osobních údajů od subjektu údajů o účelu, pro který jsou osobní údaje požadovány. Organizace nezpracovává neoprávněně žádné osobní údaje, a to ani ty, které mohou mít na subjekt údajů (fyzickou osobu) negativní vliv.

- Organizace vede jen ty osobní údaje, na které má právní nárok. Právní nároky evidence osobních údajů jsou popsány v přílohách Záznamů o činnostech zpracování pro software a dokumenty používané v organizaci.
- Pracovníci organizace v maximálně možné míře transparentně informují subjekty údajů o zpracování jejich osobních údajů a o jejich právech.
- Při zpracování se chovají pracovníci organizace korektně s ohledem na zajištění maximálního zabezpečení proti zneužití či zcizení osobních údajů subjektu údajů.
- Před zahájením zpracování nových skupin osobních údajů odpovědní pracovníci organizace ve spolupráci s pověřencem pro ochranu osobních dat prověřují pomocí všech zásad oprávněnost jejich zpracování.

Účelové omezení

Všichni pracovníci organizace zpracovávají osobní údaje subjektu údajů pouze k těm účelům, ke kterým mají právní nárok tyto zpracovávat. Účely zpracování jsou uvedeny vždy na kartě dokumentu, souboru či v databázi, které jsou součástí směrnice. Při každém zpracování nového druhu osobního údaje, či již existujícího osobního údaje k novému účelu, prověřuje organizace ve spolupráci s pověřencem pro ochranu osobních údajů účelovou oprávněnost takového zpracování.

- Organizace zpracovává osobní údaje subjektu údajů jen k těm účelům, ke kterým má právní nárok (na základě zákona, smlouvy, oprávněného nároku nebo na základě souhlasu).
- Údaje, ke kterým pozbývá právního nároku, neodkladně anonymizuje.
- Způsoby anonymizace jsou popsány v přílohách tabulek Záznamů o činnostech zpracování pro software a dokumenty používané v organizaci.

Minimalizace údajů

Organizace zpracovává osobní údaje subjektu údajů pouze v takové míře, která je nezbytně nutná pro účely, pro které má oprávnění tyto údaje zpracovávat. U každého nového osobního údaje je posuzováno, zda je tento údaj nezbytný pro zpracování k těm účelům, na které organizace má právní nárok.

- Organizace zpracovává osobní údaje pouze v nezbytně nutném rozsahu, ke kterému má právní nárok (na základě zákona, smlouvy, oprávněného nároku nebo na základě souhlasu).
- Jednotlivé zpracovávané osobní údaje a jejich skupiny jsou popsány v přílohách tabulek Záznamů o činnostech zpracování pro software a dokumenty používané v organizaci.

Přesnost

Odpovědní pracovníci organizace ověřují, že osobní údaje, které jsou zpracovávány, jsou přesné. Ověřování se provádí při přijímání jak nových osobních údajů od již evidovaných subjektů údajů, tak i osobních údajů od nových subjektů údajů. V případě, že organizace zjistí, že zpracovává nepřesné údaje, tyto po ověření neodkladně opraví.

- Při získávání osobních údajů od subjektu údajů prověřují pracovníci organizace jejich přesnost a pravdivost. Ověřování pravdivosti a přesnosti údajů probíhá osobním, písemným nebo telefonickým kontaktem s fyzickou osobou.
- V případě, že jsou zjištěny nepřesné nebo nepravdivé údaje o subjektu údajů, jsou tyto údaje neprodleně po ověření pravdivosti opraveny.
- Po dobu ověření jejich pravdivosti neprovádí správce žádné zpracování nad osobními údaji.
- Pokud má organizace povinnost předávat osobní údaje fyzické osoby dalším příjemcům, neodkladně informuje o takto provedené změně i další příjemce.

Omezení uložení

Organizace zpracovává jen ty osobní údaje, ke kterým má oprávnění a jen po dobu, po kterou má k jejich zpracování právní nárok. Po ukončení doby, po kterou má organizace k jejich zpracování právní nárok, dochází k anonymizaci těchto osobních údajů.

- Zpracování osobních údajů je jen po dobu, po kterou má organizace právní nárok na jejich zpracování. Podrobněji je právní nárok popsán v Záznamech o činnostech zpracování pro software a dokumenty používané v organizaci.
- Způsoby anonymizace jsou popsány v kapitole způsoby ochrany osobních údajů.
- Doba, po kterou má organizace právní nárok na vedení určité skupiny osobních údajů, je popsána v Záznamech o činnostech zpracování pro software a dokumenty používané v organizaci.

Integrita a důvěrnost

Všechny osobní údaje jsou v organizaci zpracovávány takovým způsobem, který zajistí jejich náležité zabezpečení před neoprávněným, či protiprávním zpracováním, či před náhodnou ztrátou. Způsoby zabezpečení jsou konkretizovány v samostatné kapitole.

- Zajištění bezpečnosti zpracovávaných osobních údajů je popsáno v přílohách Záznamů o činnostech zpracování pro software a dokumenty používané v organizaci.

Odpovědnost

Organizace se chová maximálně odpovědně k dodržování všech zásad ochrany osobních údajů. Pracovníci organizace aktivně spolupracují s vedením a pověřencem pro ochranu osobních dat v aktivním předcházení ztrátě, zničení či poškození osobních dat subjektu údajů.

E. Zpracování osobních údajů

Organizace zpracovává osobní údaje fyzických osob dle zásad nařízení Evropského parlamentu a Rady (EU) číslo 2016/679 a podle zákona č. 110/2019 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Jednotlivé druhy zpracování osobních údajů, včetně jejich zabezpečení, jsou podrobně uvedeny v Záznamech o činnostech na konci této směrnice.

F. Způsoby ochrany osobních údajů

Organizace zajišťuje nejvyšší možnou ochranu osobních údajů subjektů údajů podle jejich povahy v elektronické nebo písemné podobě.

Písemná podoba – dokumenty obsahující osobní údaje – v produkčním prostředí

- Dokumenty obsahující osobní data, jsou v kancelářích uzavřeny v uzamykatelných skříních.
- Do kanceláří a uzamykatelných skříní má přístup pouze odpovědná osoba seznámená s ochranou osobních údajů.
- Dokumenty obsahující osobní data nejsou poskytovány žádné další osobě, která nemá právo na nahlížení k těmto datům ani nemá právo s nimi dále pracovat.
- Odpovědné osoby jsou seznámeny s pravidly ochrany osobních údajů v organizaci. Při předávání osobních údajů jiným pracovníkům v organizaci či mimo organizaci se chovají maximálně odpovědně. Při každém takovém předávání osobních údajů předem prověřují, zda příjemce osobních údajů má na tyto informace právní nárok.
- Předávání osobních údajů fyzických osob i mimo ni se řídí zásadami popsány v kapitole Předávání osobních údajů jiným příjemcům/zpracovatelům.

Písemná podoba – dokumenty obsahující osobní údaje – spisovna (archiv)

- Archivní dokumenty obsahující osobní data jsou uzavřeny v samostatné místnosti (spisovně) organizace, která je zajištěna proti vniknutí osobám, které k tomu nemají oprávnění.
- Spisovna je zajištěna před poškozením v něm uložených dokumentů proti požáru a dalším vnějším vlivům, které mohou znehodnotit takto uložené dokumenty.
- Po ukončení platnosti dokumentů nebo doby, po kterou dokumenty mohou být v organizaci uloženy, jsou tyto dokumenty skartovány dle skartačního a spisového řádu. Skartaci dokumentů provádí organizace sama. Ostatní dokumenty, nepodléhající skartaci, jsou předány do státního archivu v Náchodě.
- Je vedena evidence všech dokumentů, které jsou ve spisovně uloženy a to i těch, které byly skartovány či předány do centrálního archivu.

Elektronická podoba – data obsahující osobní data – produkční databáze a soubory

- Elektronické soubory s osobními daty jsou uloženy na zabezpečeném společném datovém uložišti (datovém serveru), kam mají přístup jen oprávnění pracovníci organizace. Elektronické soubory s osobními daty jsou v maximálně možné míře zajištěny proti zcizení, zničení, vnějším hrozbám a jinému neoprávněnému zpracování.
- Přístupy do informačních systémů obsahujících osobní data jsou zajištěny hesly obsahujícími minimálně alfanumerické znaky a číslice v délce 6 znaků. Přístupy do systémů mají pouze oprávnění pracovníci, kteří mohou zpracovávat osobní data subjektu údajů.
- Každý počítač je jistěn uživatelským heslem obsahujícím minimálně alfanumerické znaky a číslice v délce 6 znaků.
- Při vzdálení se od PC je pracovník povinen zamknout tento PC klávesovou zkratkou Windows klávesa + L.
- Pracovníci, kteří přicházejí do styku s osobními daty v informačních systémech, mají zajištěn sledovaný přístup s možností exportu do obecných formátů MS Excel, Word, Acrobat Reader. O jednotlivých exportech dat je vedena elektronická evidence přímo v informačním systému. Tato funkcionality zajišťuje zpětnou kontrolu o tom, kdo, kdy a co exportoval a k jakému účelu. Tuto funkcionality mají zprovozněnu pracovníci pouze v informačních systémech nabízejících tuto možnost. Bližší výpis těchto informačních systémů je popsán v kapitole Záznamy o činnostech.
- Odpovědní pracovníci organizace, kteří přicházejí do styku s osobními údaji v elektronické podobě, jsou seznámeni s tím, že bez svolení vedení organizace nebudou tato data za žádných okolností ukládat, duplikovat či zálohovat do jiných než předem schválených umístění.
- Datový server (společné datové uložště) proti vnějším hrozbám je chráněn bránou Firewall. Na PC stanicích i datovém serveru je instalován pravidelně aktualizovaný antivirový program.

Elektronická podoba – data obsahující osobní data – archivní databáze a soubory

- Soubory a databáze s osobními daty jsou pravidelně 1x měsíčně zálohovány na zabezpečené uložení. Tyto zálohy dat jsou využívány pro případ obnovy po havárii produkčních dat. Po obnově dat z těchto záloh jsou nejprve osobní data aktualizována na poslední známý stav a teprve po tomto kroku jsou data uvolněna k dalšímu zpracování.
- Zabezpečené uložení pro produkční zálohy elektronických dat, obsahujících mimo jiné i osobní údaje subjektu údajů, se nachází technicky na datovém serveru organizace nebo na vzdáleném uložení v cloudu případně i na externím zařízení připojeném k datovému serveru organizace.
- K zálohám produkčních databází a souborů má přístup pouze k tomu pověřená osoba, zpravidla správce IT a jeho zástupce.
- Pověřená osoba k provádění záloh má na odpovědnost provádění kontrol produkčních záloh v takové míře, aby zajistila jejich neměnnost, nezcizitelnost, správnost a ochranu před zničením. Kontrolu správnosti provádění záloh zajišťuje zpravidla v časovém úseku každé 3 měsíce.
- V případě, že se provádí záloha produkčních dat do uložení, které není pod správou organizace, má zajištěno pod smlouvou garanci zajištění bezpečnosti uložených dat od zpracovatele.
- Zabezpečené uložení s osobními daty je v maximálně možné míře zajištěno proti jejich zcizení, zničení, vnějším hrozbám a jinému neoprávněnému zpracování.
- Provádění produkčních záloh elektronických souborů s osobními daty je pouze na uložení k tomu předem určená pod kontrolou odpovědného pracovníka, správce IT.

G. Způsoby anonymizace po ukončení doby zpracování osobních údajů

Organizace provádí řízenou anonymizaci osobních údajů ve všech informačních systémech, které zpracovávají osobní data, a které obsahují tuto funkcionalitu. Výsledkem anonymizace je nevratná změna osobních údajů subjektu bez možnosti jejich zpětné obnovy, která povede k dohledání skutečné osoby. Anonymizace se provádí po ukončení všech oprávněných nároků organizace na zpracovávání osobních údajů fyzické osoby.

- Anonymizace osobních údajů se provádí v informačních systémech, které tuto funkcionalitu nabízejí, uvedených v Záznamech o činnostech na konci této směrnice.
- Anonymizace ostatních osobních údajů uložených v ostatních informačních systémech (které možnost automatické anonymizace nenabízejí) nebo souborech provádí pracovník organizace manuálně podle zásad GDPR. Zpravidla hodnoty v osobních údajích vymaže nebo přepíše na hodnotu, která nevyjadřuje konkrétní fyzickou osobu.
- Anonymizace písemných dokumentů je provedena formou nevratného přemazání osobních údajů subjektu, které vede k tomu, že daná osoba není zpětně identifikovatelná.
- Samostatným způsobem anonymizace je skartace listinného dokumentu po době právního nároku nebo výmaz elektronického souboru.

H. Způsoby pseudonymizace osobních údajů

Organizace nemá dostupné technické prostředky ani personální kapacity, které umožňují provádět nad daty jejich řízenou pseudonymizaci. Organizace zajišťuje ochranu osobních dat pomocí jiných nástrojů, než je právě způsob zabezpečení formou pseudonymizace.

I. Způsoby předávání osobních údajů v rámci organizace

V rámci organizace se předávají dokumenty s osobními daty pouze mezi pracovníky, kteří mají oprávnění zpracovávat tyto osobní údaje. Tyto dokumenty a elektronická data jsou vždy zajištěny tak, aby se k nim nemohla dostat pro toto zpracování neoprávněná osoba.

Dokumenty a osobní data v elektronické podobě jsou sdíleny na společném zabezpečeném uložišti organizace, kam mají přístup pouze pracovníci oprávnění ke zpracování těchto osobních údajů.

Pokud se osobní údaje fyzických osob zasílají mezi pracovníky organizace pomocí elektronické pošty, jsou tyto údaje vždy umístěny v příloze, která je zašifrována. Způsob šifrování je uveden v samostatné kapitole této směrnice. Heslo k šifrované příloze si pracovníci předávají jinou cestou než v zaslané zprávě.

J. Způsoby předávání osobních údajů jiným zpracovatelům

Organizace předává osobní údaje jiným zpracovatelům pouze v nezbytně nutné míře pro účely, které není schopna samostatně vykonávat. Soupis předávaných osobních údajů a seznam zpracovatelů je uveden na konci této směrnice v příloze Záznamy o činnostech.

Listinné dokumenty jsou předávány proti podpisu zástupce zpracovatele či jinému potvrzení, které zajišťuje, aby se k dokumentu nedostala neoprávněná osoba.

Elektronické dokumenty se předávají v podobě, která zajišťuje, aby se k datům nedostala nepovolaná osoba. Pokud je to možné, jsou veškerá takto předávaná data šifrována.

- Zasílání dokumentů a souborů, které obsahují osobní data, je prováděno na úřady státní správy vždy formou zabezpečené zprávy pomocí datových schránek.
- Zasílání dokumentů a souborů, které obsahují osobní data, může být prováděno ostatním zpracovatelům pomocí e-mailové korespondence, kdy je příloha vždy šifrována a zajištěna proti neoprávněnému zpracování heslem. Heslo je po dohodě zasíláno samostatnou sms zprávou na mobilní telefon příjemce zprávy nebo je dohodnuto mezi příjemcem a odesílatelem jinou cestou (uvedeno smluvně, telefonickým rozhovorem apod.). V případě zasílání zpracovatelům z oblasti státní správy jsou vždy dokumenty zasílány formou zprávy pomocí služby datové schránky od provozovatele Česká pošta.
- Zasílání zpráv formou e-mailové korespondence je prováděno pouze na ověřené adresy zpracovatele.
- Heslo, které zajišťuje bezpečnost přílohy s obsahem osobních dat, může být po dohodě správce a zpracovatele používáno shodné pro více dokumentů.

K. Způsoby předávání osobních údajů dalším příjemcům

Organizace předává osobní údaje příjemcům pouze v takové míře, kterou stanovuje příslušný předpis či zákon.

Listinné dokumenty jsou předávány proti podpisu zástupce příjemce či jinému potvrzení, které zajišťuje, aby se k dokumentu nedostala neoprávněná osoba.

Elektronické dokumenty se předávají v podobě, která zajišťuje, aby se k datům nedostala nepovolaná osoba. Pokud je to možné, jsou veškerá takto předávaná data šifrována.

- Zasílání dokumentů a souborů, které obsahují osobní data, je prováděno na úřady státní správy vždy formou zabezpečené zprávy pomocí datových schránek.
- Zasílání dokumentů a souborů, které obsahují osobní data, může být prováděno ostatním příjemcům pomocí e-mailové korespondence, kdy je však příloha vždy šifrována a zajištěna proti neoprávněnému zpracování heslem. Heslo je po dohodě zasíláno samostatnou sms zprávou na mobilní telefon příjemce zprávy nebo je dohodnuto mezi příjemcem a odesílatelem jinou cestou (uvedeno smluvně, telefonickým rozhovorem apod.). V případě zasílání příjemcům z oblasti státní správy jsou vždy dokumenty zasílány formou zprávy pomocí služby datové schránky od provozovatele Česká pošta.
- Zasílání zpráv formou e-mailové korespondence je prováděno pouze na ověřené adresy příjemce.
- Heslo, které zajišťuje bezpečnost přílohy s obsahem osobních dat, může být po dohodě správce a příjemce používáno shodné pro více dokumentů.
- Správce, dat si dopředu ověří, zda má oprávnění zaslat určená osobní data příjemci.

L. Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím *(podle článku 44 nařízení GDPR a zákona č. 110/2019)*

Organizace nepředává žádné osobní údaje o subjektech údajů do třetích zemí nebo mezinárodním organizacím.

M. Zpracování osobních údajů za účelem cíleného marketingu

Organizace **nezpracovává** žádné osobní údaje za účelem cíleného marketingu. K těmto účelům proto **nepožaduje** od fyzických osob souhlas pro jejich zpracování.

N. Práva fyzických osob *(podle nařízení GDPR a zákona č. 110/2019)*

Organizace plně respektuje práva fyzických osob a tato aplikuje do pravidel zpracování a ochrany osobních údajů.

Právo subjektu údajů na přístup k osobním údajům (podle článku 15 nařízení GDPR a zákona č. 110/2019)

Organizace zajišťuje realizaci práva subjektu údajů na přístup k osobním údajům formou uvedenou v následujícím postupu:

- Organizace má stanoveného pracovníka, který eviduje a přijímá žádosti fyzických osob o výpis osobních údajů.
- Po obdržení žádosti organizace prověří totožnost žadatele a to, zda fyzická osoba má právo požadovat výpis osobních údajů. Žádost o výpis osobních údajů je přijímána jen v podobě žádosti formou elektronické pošty nebo formou písemné žádosti.
- Následně odpovědný pracovník si vyžádá ze všech oddělení v organizaci výpis osobních údajů žadatele (fyzické osoby), v rozsahu seznam osobních údajů (například jméno, příjmení, bydliště, email, telefon a další, které organizace zpracovává) a k jakým účelům a po jakou dobu budou zpracovávány. Dále zda tyto údaje jsou zpracovávány pouze v organizaci nebo předávány dalším zpracovatelům.
- Výslednou zprávu předává odpovědný pracovník žadateli v písemné podobě. Předání žadateli probíhá formou osobního předání, kdy si pracovník organizace nejprve ověří totožnost osoby, která si přijde výpis osobních údajů převzít. Poté proti podpisu je výpis osobních údajů předán. Další možností je zaslání výpisu osobních údajů formou datové zprávy pomocí služby datových schránek České pošty v případě, že datovou schránku žadatel vlastní. Poslední možností je zaslání výpisu osobních údajů žadateli formou doporučeného psaní do vlastních rukou.
- Subjekt údajů (fyzická osoba) má právo výslednou zprávu obdržet do 30 dní od data zaslání a ověření žádosti.
- Výsledná zpráva je pro subjekt údajů bezplatná.
- O veškeré komunikaci se žadatelem vede odpovědný pracovník organizace podrobnou evidenci.

Organizace může žádost zamítnout v případech, kdy je neopodstatněná, opakovaná atd. V případě, že žádost je opakovaná v době, kdy žadatel předpokládá, že nedošlo k žádné změně v jeho zpracovávaných osobních údajích, potom bude organizace požadovat za tento úkon přiměřený administrativní poplatek. O tomto organizace dopředu žadatele informuje.

- Účely zpracování osobních údajů.
- Kategorie dotčených osobních údajů.
- Příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména potom příjemci ve třetích zemích nebo v mezinárodních organizacích.
- Jaká je plánovaná doba, po kterou budou osobní údaje uloženy nebo není-li možné ji určit, kritéria použita pro stanovení této doby.
- Veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.
- Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Fyzická osoba má právo na tyto údaje, pokud je správce zpracovává:

Zajištění práva přenositelnosti subjektu údajů *(podle článku 20 nařízení GDPR a zákona č. 110/2019)*

Organizace zajišťuje právo subjektu údajů na přenositelnost osobních dat k jiným správčům. V případě, že subjekt údajů požádá organizaci o předání osobních dat pro jejich převedení jiným správčům, potom:

- Organizace ověří totožnost žadatele a zákonnost této žádosti.
- V přiměřené lhůtě, která odpovídá časové náročnosti takového úkonu, připraví opis osobních dat subjektu údajů.
- Veškerá osobní data subjektu údajů uloží do elektronického souboru v podobě formátu MS Excel, Word, Acrobat Reader a tato data proti podpisu předá žadateli v zajištěné podobě tak, aby se k nim nedostala neoprávněná osoba před jejich předáním.
- Předání osobních údajů je proti podpisu žadatele.
- O veškeré komunikaci se žadatelem vede odpovědný pracovník organizace podrobnou evidenci.

Právo fyzické osoby na opravu *(podle článku 16 nařízení GDPR a zákona č.110/2019)*

Organizace zajistí neprodlenou opravu osobních dat subjektu údajů v případě, že obdrží od fyzické osoby informace, které potvrzují nové skutečnosti v datech ve zpracovávání osobních údajích o této osobě.

- Fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které o této osobě zpracovává.
- Správce si v první řadě ověří, že osobní údaje, které fyzická osobě požaduje opravit, odpovídají skutečnosti.
- Po ověření správce provede změnu osobních údajů dle nových skutečností ve všech evidencích, které zmíněné osobní údaje obsahují.
- O výsledku opravy informuje správce žadatele formou elektronické zprávy nebo formou písemného sdělení.
- O veškeré komunikaci se žadatelem vede odpovědný pracovník organizace podrobnou evidenci.
- V případě, že organizace poskytuje osobní údaje fyzické osoby i jiným příjemcům, bez zbytečného odkladu předává tyto nové údaje i těmto příjemcům.

Právo fyzické osoby na výmaz *(podle článku 17 nařízení GDPR a zákona č. 110/2019)*

Organizace je připravena provést výmaz osobních údajů fyzické osoby na základě její žádosti v případě, že nejsou k tomuto kroku shledány právní důvody, pro které tuto operaci nelze zajistit.

- Fyzická osoba musí podat žádost na výmaz v písemné nebo elektronické podobě.
- Žádost musí obsahovat důvody fyzické osoby pro výmaz.
- Organizace ověří totožnost žadatele, fyzické osoby a ověří oprávněnost na výmaz.
- V průběhu této doby (po kterou provádí ověření oprávněnosti výmazu), organizace omezí zpracování osobních údajů žadatele.
- V případě, že žádost je oprávněná, provede organizace smazání veškerých osobních údajů žadatele ve všech evidencích, kde již nemá právní důvody pro zpracování těchto údajů fyzické osoby.
- O výsledku oprávněnosti žádosti organizace informuje žadatele v písemné podobě.
- O jednotlivých krocích a žádostech vede organizace elektronickou evidenci.

Právo na omezení zpracování *(podle článku 18 nařízení GDPR a zákona č. 110/2019)*

Organizace je připravena omezit zpracování osobních údajů subjektu údajů na základě ověřené žádosti fyzické osoby po dobu, po kterou se vyjasní důvody pro omezení zpracování.

- Fyzická osoba musí podat žádost na omezení zpracování v písemné nebo elektronické podobě.
- Žádost musí obsahovat důvody fyzické osoby pro omezení zpracování.
- Organizace ověří totožnost žadatele, fyzické osoby a ověří oprávněnost na omezení zpracování.
- V případě, že žádost je oprávněná, omezí zpracování veškerých osobních údajů žadatele ve všech evidencích, kde se taková data nacházejí.
- V průběhu této doby posoudí organizace žádost a provede (či ne) nápravná opatření v takové míře, která zajistí pominutí důvodu k omezení zpracování na straně organizace.
- O výsledku těchto opatření organizace informuje žadatele.
- V případě, že pominou důvody k omezení zpracování, organizace obnoví zpracování osobních dat subjektu údajů.
- O jednotlivých krocích a žádostech vede organizace elektronickou evidenci.

O. Hlášení bezpečnostních incidentů *(podle článku 33 nařízení GDPR a zákona č. 110/2019)*

V případě, že dojde v organizaci k porušení bezpečnosti zpracovávaných osobních dat, které může mít za následek poškození práv a svobod osob subjektu údajů, vedení organizace tento incident ve spolupráci s pověřencem pro ochranu osobních údajů (DPO) nahlásí na Úřad pro ochranu osobních údajů.

Zpráva musí mít tyto náležitosti:

- Popis povahy daného případu porušení bezpečnosti zajištění osobních dat subjektu údajů.
- Popis pravděpodobných důsledků porušení zabezpečení osobních údajů.
- Datum a čas vzniku incidentu.
- Popis opatření, které organizace přijala nebo navrhla k přijetí s cílem vyřešit dané porušení v podobě zabezpečení osobních údajů.
- Jméno a kontaktní údaj na Pověřence pro ochranu osobních údajů (DPO).

Nahlášení bezpečnostního incidentu musí organizace nahlásit nejpozději do 72 hodin od vzniku incidentu.

P. Stanovení Pověřence pro ochranu osobních údajů (DPO) *(podle článku 37 nařízení GDPR a zákona č. 110/2019)*

Organizace jmenuje „Pověřencem pro ochranu osobních údajů“ (DPO) osoby:

Jméno: Tomáš Urban

Společnost: Softbit software, s.r.o.

Telefon: 603 449 244

E-mail: tomas.urban@softbit.cz

Správce či zpracovatel informuje pověřence pro ochranu osobních údajů s předstihem o všech skutečnostech v souvislosti se zpracováním osobních údajů v organizaci. V součinnosti oba řeší případně změny ve zpracování osobních údajů podle všech zásad dle nařízení GDPR a povinnosti správce či zpracovatele.



- Pověřenec pro ochranu osobních údajů zajišťuje poskytování veškerých informací a poradenství správci a dalším zpracovatelům a pracovníkům v oblasti ochrany osobních údajů fyzických osob.
- Pověřenec pro ochranu osobních údajů provádí školení pracovníků organizace.
- Monitoruje provádění ochrany osobních údajů fyzických osob v organizaci v souladu s nařízením GDPR a zákonem č. 110/2019 formou kontrol.
- Spolupracuje jménem organizace s Úřadem pro ochranu osobních údajů.
- Působí jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování osobních údajů v organizaci.
- Pověřenec pro ochranu osobních údajů rovněž zajišťuje práva fyzických osob podle nařízení GDPR a spolupracuje v oblasti těchto práv se správcem.

Q. Školení pracovníků, kteří přicházejí do styku s osobními údaji

Organizace provádí pravidelná školení všech pracovníků, kteří přicházejí do styku s osobními údaji subjektu údajů tak, aby zajistila soulad s nařízením GDPR, zákonem č. 110/2019 a směrnicí GDPR pro příspěvkovou organizaci.

- Pracovníci, kteří přicházejí do styku s osobními údaji, zachovávají plnou mlčenlivost ve vztahu k jiným osobám a organizacím, které nemají žádný právní nárok tyto informace požadovat a to i po ukončení jejich pracovního poměru v organizaci.
- Noví pracovníci organizace mají povinnost se seznámit s touto směrnicí při svém nástupu do pracovního poměru, porozumět ji a řídit se všemi pravidly v ochraně osobních údajů uvedenými v této směrnici
- V případě jakýchkoli nejasností s ochranou osobních údajů fyzických osob mohou všichni pracovníci organizace požádat pověřence k ochraně osobních údajů o jejich vysvětlení.

R. Oddělení v organizaci, která se řídí směrnicí

V organizaci se řídí nařízením k GDPR o ochraně osobních údajů fyzických osob, zákonem č. 110/2019 a směrnicí GDPR pro příspěvkovou organizaci k tomuto nařízení tato oddělení:

Ředitel(ka) organizace Ekonomické a účetní oddělení Mzdová účtárna a personální oddělení
--

Směrnice nabývá účinnost dne 01.05.2025

Podpis ředitele (jednatele) organizace:	
Podpis pověřence pro ochranu osobních dat:	

Udělení souhlasu s poskytnutím osobních údajů

Správce osobních údajů : **Mateřská škola, Náchod, Vítkova 304, IČo: 70996458**

Já pan (paní), zákonný zástupce dítěte dávám výslovný souhlas správci osobních údajů ke zpracování těchto osobních údajů o mém dítěti, a to pro účel(y):

1. Uvádění jména a příjmení dítěte na seznámech pro organizování mimoškolních akcí (výletů, divadelní představení, kino, sportovní aktivity, muzikoterapie, canisterapie, vzdělávací akce)

Udělují souhlas k účelu dle bodu 1

podpis:.....

2. Poskytování jména a příjmení dítěte jiným zpracovatelům při organizování mimoškolních akcí (plavání, lyžování, bruslení)

Udělují souhlas k účelu dle bodu 2

podpis:.....

3. Evidence jména a příjmení osob, které budou odvádět dítě z mateřské školy

Udělují souhlas k účelu dle bodu 3

podpis:.....

4. Fotografování dítěte za účelem propagace MŠ, akcí v MŠ, zveřejnění fotografie v tisku, na webových stránkách školy, pro účely dokumentace školy

Udělují souhlas k účelu dle bodu 4

podpis:.....

5. Prezentace písemností a jiné projevy osobní povahy dítěte za účelem propagace školy a informování o aktivitách školy (výtvarné práce na nástěnkách školy, výstavách, hudební vystoupení)

Udělují souhlas k účelu dle bodu 5

podpis:.....

Body 1 – 3 tohoto souhlasu platí po dobu docházky dítěte do organizace správce, body 4 a 5 platí po dobu existence organizace. Byl(a) jsem poučen(a) o svém právu tento souhlas kdykoliv bez udání důvodu písemně odvolat. Správce osobních údajů je povinen zrušení tohoto souhlasu k účelům, ke kterým byl udělen, bezodkladně provést. Odvoláním souhlasu však není dotčena zákonnost zpracování osobních údajů v organizaci po dobu platnosti souhlasu.

Souhlas je vyjádřením svobodného rozhodnutí fyzické osoby a není podmínkou pro zajištění ostatních služeb ze strany organizace.

Dne:

Podpis zákonného zástupce dítěte:

Zrušení uděleného souhlasu k poskytnutí osobních údajů

Správce osobních údajů : **Mateřská škola, Náchod, Vítkova 304, IČo: 70996458**

Já pan (paní), zákonný zástupce dítěte ruším
výslovný souhlas správci osobních údajů ke zpracování těchto osobních údajů o mém dítěti, a to pro účel(y):

1. Uvádění jména a příjmení dítěte na seznámech pro organizování mimoškolních akcí (výletů, divadelní představení, kino, sportovní aktivity, muzikoterapie, canisterapie, vzdělávací akce)

Ruším souhlas k účelu dle bodu 1

podpis:.....

2. Poskytování jména a příjmení dítěte jiným zpracovatelům při organizování mimoškolních akcí (plavání, lyžování, bruslení)

Ruším souhlas k účelu dle bodu 2

podpis:.....

3. Evidence jména a příjmení osob, které budou odvádět dítě z mateřské školy

Ruším souhlas k účelu dle bodu 3

podpis:.....

4. Fotografování dítěte za účelem propagace MŠ, akcí v MŠ, zveřejnění fotografie v tisku, na webových stránkách školy, pro účely dokumentace školy

Ruším souhlas k účelu dle bodu 4

podpis:.....

5. Prezentace písemností a jiné projevy osobní povahy dítěte za účelem propagace školy a informování o aktivitách školy (výtvarné práce na nástěnkách školy, výstavách, hudební vystoupení)

Ruším souhlas k účelu dle bodu 5

podpis:.....

Správce osobních údajů je povinen zrušení tohoto souhlasu k účelům, ke kterým byl udělen, bezodkladně provést. Odvoláním souhlasu však není dotčena zákonnost zpracování osobních údajů v organizaci po dobu platnosti souhlasu.

Dne:

Podpis zákonného zástupce dítěte:

Příloha č. 1: Udělení souhlasu s poskytnutím osobních údajů**Správce**

Název organizace:	
IČO:	DIČ:

Subjekt údajů / Fyzická osoba

Jméno a příjmení:	
Bydliště:	
Doklad totožnosti:	

Já, výše uvedená fyzická osoba, tímto uděluji souhlas se zpracováním osobních údajů v rozsahu:

Jméno a příjmení:	
Bydliště:	
Průkaz totožnosti:	
Telefon:	
E-mail:	
Další...:	

Pro účel:

--

Na dobu:

Určitou od – do
Neurčitou

Fyzická osoba může zrušit svůj souhlas se zpracováním výše uvedených osobních údajů kdykoli, a to písemným sdělením. Správce je povinen zrušením tohoto souhlasu k účelům, ke kterým byl udělen, bezodkladně provést. Odvoláním souhlasu však není dotčena zákonnost zpracování v organizaci po dobu platnosti souhlasu.

Souhlas je vyjádřením svobodného rozhodnutí fyzické osoby a není podmínkou pro zajištění ostatních služeb ze strany organizace k subjektu údajů.

Subjekt údajů / Fyzická osoba

.....

(čitelný podpis, datum)

Příloha č. 2: Zrušení uděleného souhlasu k poskytnutí osobních údajů**Správce**

Název organizace:	
IČO:	DIČ:

Subjekt údajů / Fyzická osoba

Jméno a příjmení:	
Bydliště:	
Doklad totožnosti:	

Já, výše uvedená fyzická osoba, tímto ruším svůj souhlas se zpracováním osobních údajů v rozsahu:

Jméno a příjmení:	
Bydliště:	
Průkaz totožnosti:	
Telefon:	
E-mail:	
Další...:	

Udělený souhlas ruším pro tyto účely:

--

Subjekt údajů / Fyzická osoba

.....

(čitelný podpis, datum)

Příloha č. 3: Karta evidovaných osobních údajů v organizaci o subjektu údajů/ fyzické osobě

Správce

Název organizace:	
IČO:	DIČ:

Subjekt údajů / Fyzická osoba

Jméno a příjmení:	
Bydliště:	
Doklad totožnosti:	

Seznam (kategorie) evidovaných osobních údajů

--

Údaje se zpracovávají pro účely

--

Údaje jsou zpracovávány podle předpisů – zákonů / po plánovanou dobu

--	--

Seznam osobních údajů, které se předávají dalším zpracovatelům či příjemcům (jakým)

--	--

Informace o zdrojích osobních údajů, pokud nejsou získány od subjektu údajů

--

Dochází k automatickému rozhodování včetně profilování (Ano/Ne)? Pokud ano, k jakému?

--

Správce předává subjektu údajů (fyzické osobě) kartu zpracovávaných osobních údajů podle nařízení GDPR o ochraně osobních údajů fyzických osob ke dni

Fyzická osoba požádala o výpis osobních údajů dne:

Správce

Subjekt údajů / Fyzická osoba

.....
(čitelný podpis, datum)

.....
(čitelný podpis, datum)

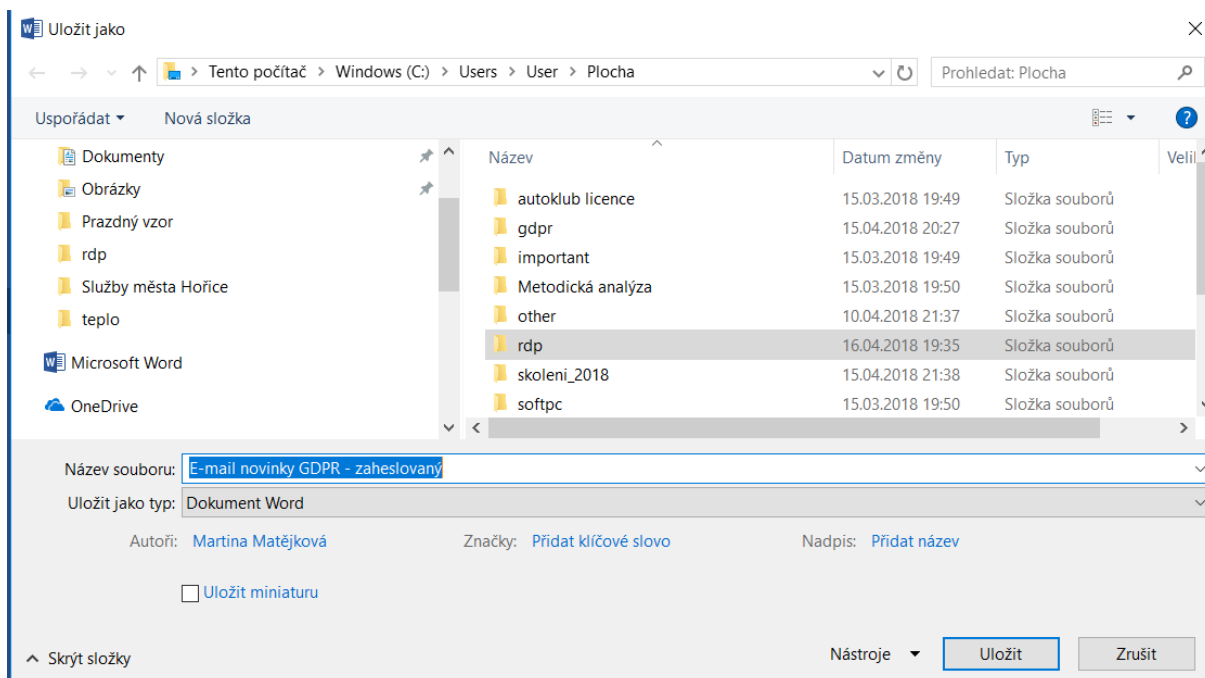
Příloha č. 4: Varianta zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem

Jednou z variant, jak mohou pracovníci organizace zabezpečit elektronický soubor pro jeho zaslání elektronickou poštou příjemci tak, aby nedošlo k jeho neoprávněnému zpracování, je možnost doplnění hesla pro otevření takového souboru.

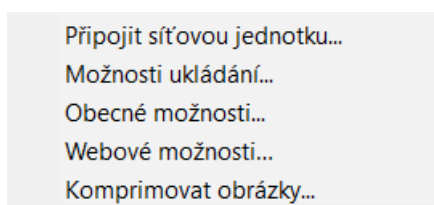
Tuto funkci podporují například kancelářské programy MS Word nebo MS Excel, ale i jiné.

V následujícím návodu si popíšeme doplnění hesla k elektronickému souboru v prostředí MS Office.

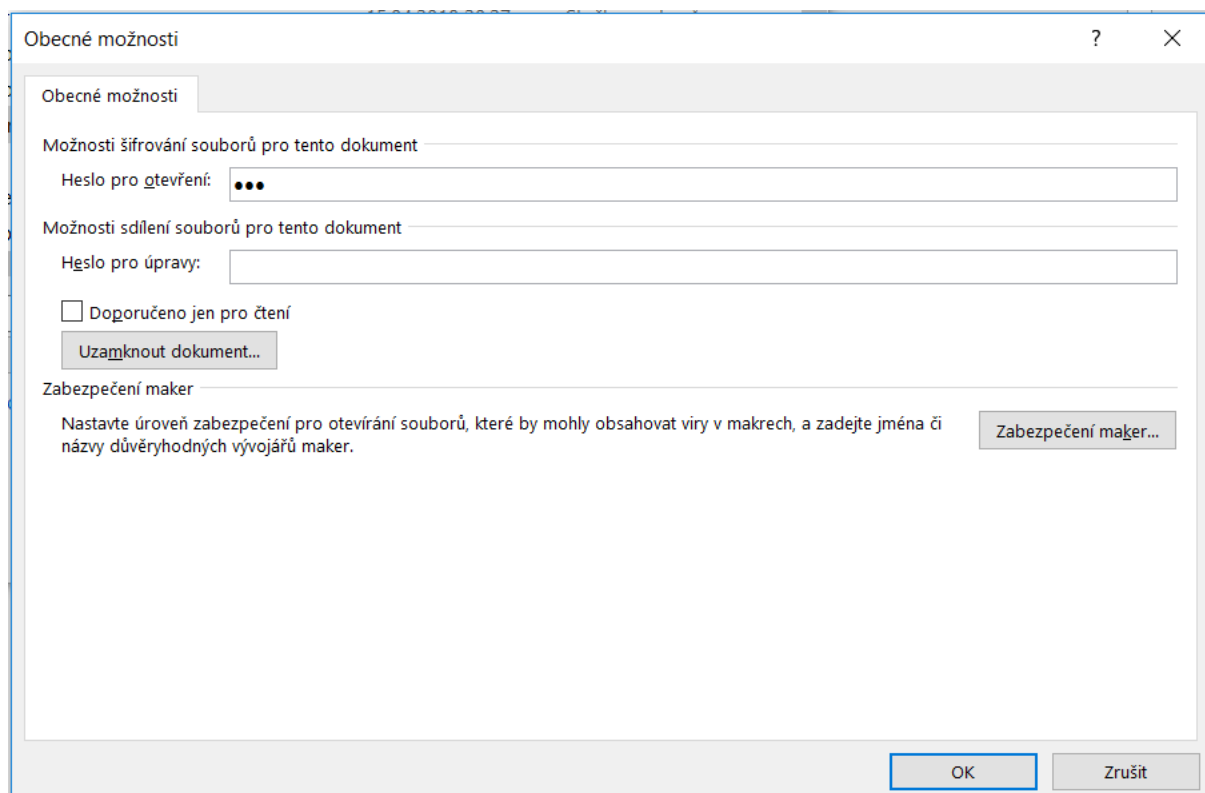
1. Vytvořený soubor uložíme přes funkci „Uložit jako“. Při ukládání zadáme název souboru s odlišným názvem než je původní, který si ponecháme ve svém počítači (tento zpravidla nebudeme doplňovat heslem pro jeho otevření).
2. Zvolíme nabídku „Nástroje“ a zde vybereme funkci „Obecné možnosti“.
3. V údají „Heslo pro otevření“ doplníme heslo, kterým chceme zabezpečit soubor pro jeho zaslání elektronickou poštou.
4. Heslo, které doplníme do souboru, zašleme příjemci jinou cestou než formou elektronické zprávy (například SMS atd.)



Obrázek 1: Uložení souboru pod jiný název ve svém PC



Obrázek 2: Výběr nabídky „Nástroje“ a zde zvolení funkce „Obecné možnosti“



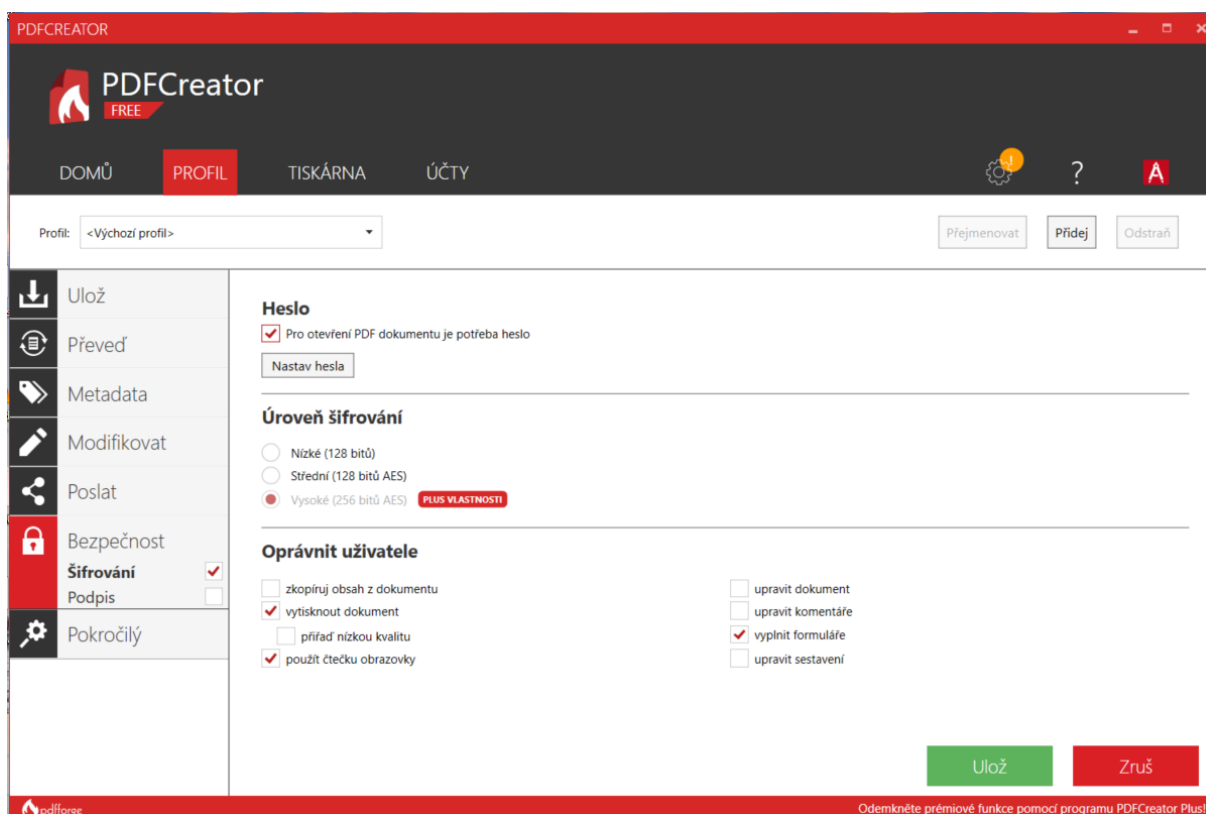
Obrázek 3: Doplnění hesla do údaje „Heslo pro otevření“ a potvrzení tlačítkem „OK“

Příloha č. 5: Varianta zabezpečení odesílaných příloh elektro. poštou – doplnění souboru heslem – PDF

U opatření PDF dokumentů heslem je nutné mít zakoupenou plnou verzi programu Acrobat Reader. Pokud tuto verzi nevlastníme, je možné opatřit PDF dokument heslem i jiným způsobem. Ve většině případů však generujeme PDF dokument z jiného formátu, například z Wordu, tiskové sestavy programu apod.

V takovém případě nám pomohou některé generátory (převodní programy) do PDF z jiných formátů. Jedním z nich je i PDF Creator.

Aby se PDF Creator při tvorbě PDF dokumentu ptal na heslo, musí být v nastavení zaškrtnuta právě možnost vložení hesla. Viz. obrázek číslo 1.



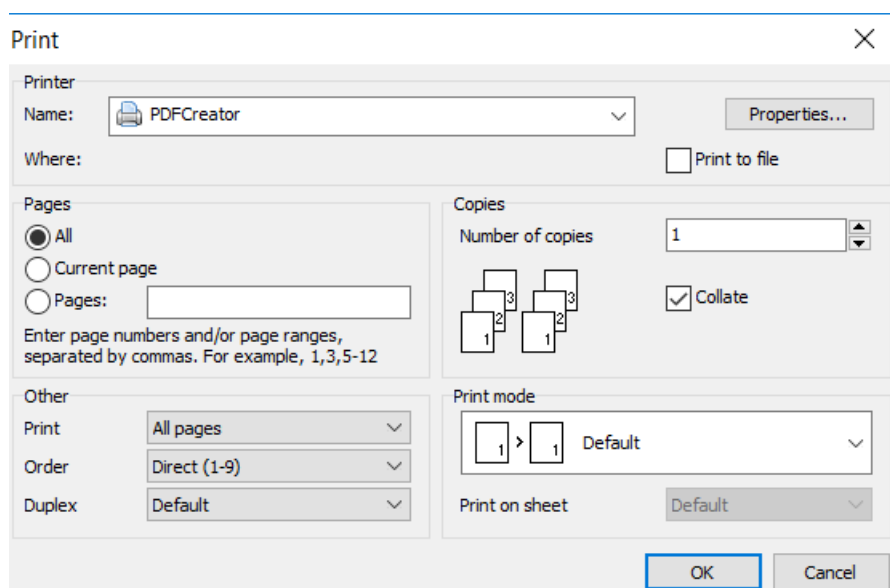
Obrázek 1: Nastavení možnosti vložení hesla

Postup opatření PDF dokumentu heslem je následující:

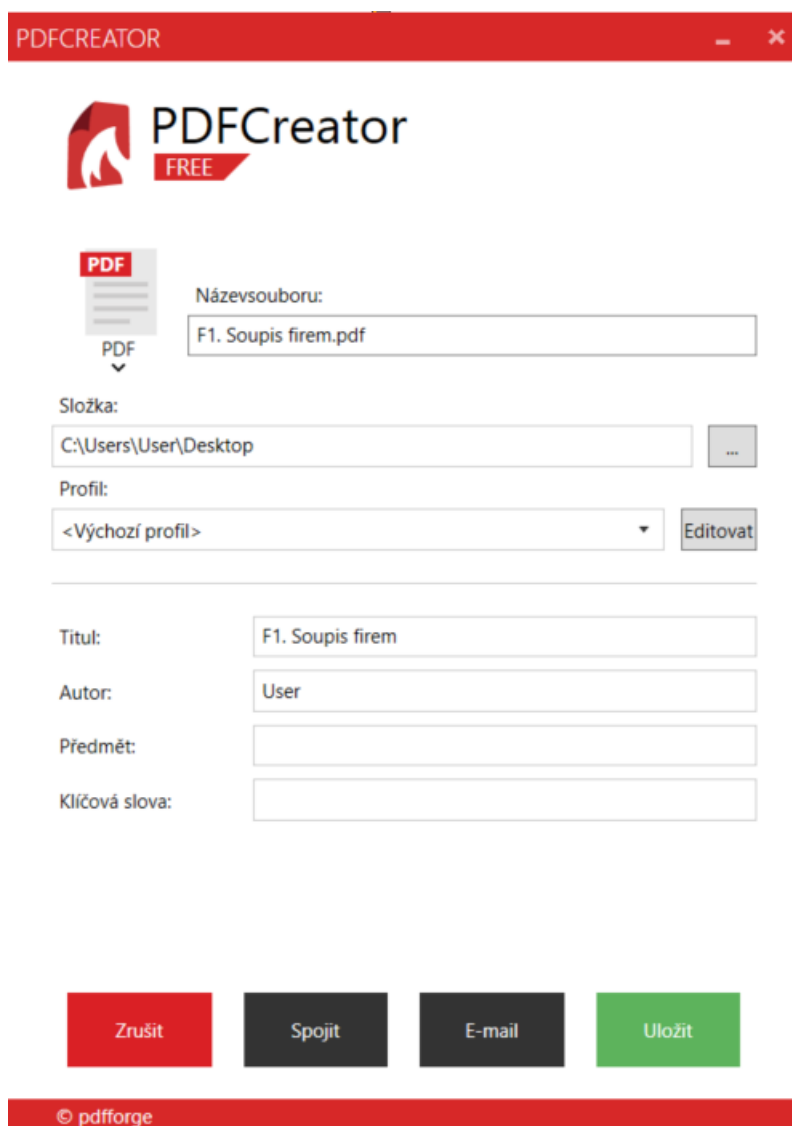
- ➔ Vytvoříme dokument ve Wordu nebo přímo tiskovou sestavu v libovolném programu.
- ➔ Zvolíme tlačítko tisk a vybereme název tiskárny PDF Creator viz. obrázek číslo 2.
- ➔ Vybereme složku, kam chceme dokument uložit a název dokumentu a zvolíme tlačítko „Uložit“ viz. obrázek číslo 3.
- ➔ Podle obrázku číslo 4 máme možnost stanovit heslo pro otevření a zvolíme tlačítko „Souhlasím“.

Tímto způsobem můžeme zasílat zaheslované soubory v PDF formátu bezpečně pomocí e-mailové pošty jiným příjemcům. Samozřejmě heslo posíláme jinou cestou.

Upozorňujeme, že grafické provedení zobrazených obrázků může být i jiné podle toho, jakou verzi PDF Creatoru vlastníte.



Obrázek 2: Výběr tiskárny PDF Creator



Obrázek 3: Uložení dokumentu

The image shows a screenshot of the PDFCreator application's security dialog box. The window has a red title bar with the text "PDFCREATOR" and standard window control buttons. Inside the window, the PDFCreator logo (a red flame icon) and the text "PDFCreator FREE" are displayed. Below this, the heading "Bezpečnost" (Security) is shown. There are two password input fields: "Vlastníkové heslo (k úpravě):" (Owner's password (for editing):) and "Uživatelovo heslo (k otevření):" (User's password (for opening):). Both fields contain three dots, indicating masked input. At the bottom of the dialog, there are three buttons: "Souhlasím" (I agree) in green, "Přeskoč" (Skip) in dark gray, and "Zruš" (Cancel) in red. The footer of the window shows the copyright notice "© pdfforge".

PDFCREATOR

 PDFCreator
FREE

Bezpečnost

Vlastníkové heslo (k úpravě):

Uživatelovo heslo (k otevření):

Souhlasím Přeskoč Zruš

© pdfforge

Obrázek 4: Stanovení hesla pro otevření dokumentu

Příloha č. 6: Vzor ohlášení dozorovému úřadu

Správce

Název organizace:

IČO:

DIČ:

Úřad pro ochranu osobních údajů

Pplk. Sochora 27

170 00 Praha 7

Věc: Ohlášení případu porušení zabezpečení osobních údajů

V souladu s ustanovením článku 33 Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) tímto ohlašuji Úřadu pro ochranu osobních údajů, že došlo k následujícímu porušení zabezpečení osobních údajů:

.....

Porušením zabezpečení osobních údajů je dotčeno celkem subjektů údajů, přičemž se jedná o následující subjekty údajů (resp. jejich kategorie):

.....

Pravděpodobné důsledky porušení zabezpečení osobních údajů jsou následující:

.....

S cílem vyřešit dané porušení zabezpečení osobních údajů a zmírnit možné nepříznivé dopady pro subjekty údajů bylo přijato nebo navrženo k přijetí následující opatření:

.....

Kontaktním místem, kde může Úřadu pro ochranu osobních údajů zjistit bližší informace ohledně výše popsaného porušení zabezpečení osobních údajů, je:

.....

V dne

.....

Záznam o činnostech zpracování – informační systémy – vzor

Informační systém (jméno a výrobce)	<i>Jméno systému a jeho výrobce</i>
Popis softwaru	<i>Popis obsahu softwaru, k čemu je určen</i>
Modul	<i>Jméno jednotlivých modulů (pokud je systém členěn do více modulů)</i>
Osobní údaje – základní	<i>Seznam základních osobních údajů, které jsou zpracovávány, např. jméno, příjmení, bydliště, datum narození, rodné číslo, e-mail, telefon</i>
Osobní údaje – ostatní	<i>Seznam ostatních osobních údajů, například národnost, věk, pohlaví</i>
Osobní údaje – citlivé	<i>Seznam osobních údajů – citlivé, například zdravotní dokumentace, finanční situace</i>
Povinnost zpracovávat údaje na základě právního nároku	<i>Na základě jakého předpisu, zákona, smlouvy organizace zpracovává osobní údaje</i>
Povinnost zpracovávat údaje po dobu podle právního nároku	<i>Po jak dlouhou dobu může organizace zpracovávat osobní údaje na základě výše uvedeného předpisu, zákona, smlouvy</i>
Evidence údajů nad právní rámec	<i>Zda se evidují osobní údaje nad právní rámec výše uvedený na základě souhlasu</i>
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	<i>Bude vyžadován souhlas?</i>
Předávání údajů do jiných systémů v rámci organizace – způsob	<i>Zda se data exportují a předávají do jiných systémů v rámci organizace</i>
Možnosti exportů dat ze systému	<i>Zda a jaké možnosti exportů dat do jiných formátů dovoluje software</i>
Předávání údajů jiným zpracovatelům	<i>Zda a jakým zpracovatelům jsou osobní data ze systému předávána, např. externí účetní</i>
Předávání údajů jiným příjemcům	<i>Zda a jakým příjemcům jsou osobní data ze systému předávána, např. ZP, OSSZ, jiný správní orgán</i>
Předávání osobních údajů do jiných zemí	<i>Zda se předává do jiných zemí</i>
Způsob zabezpečení proti zneužití	<i>Přístupy, zajištění dat, zajištění exportů dat či přenosu do jiných systémů</i>
Zálohování dat a jejich zabezpečení	<i>Jak jsou tvořeny zálohy, kde jsou ukládány a v jakém tvaru, jak jsou zabezpečeny</i>
Pracovní pozice s právem přístupu k osobním údajům	<i>Který pracovník(ce) má přístup k datům a v jaké úrovni (čtení, vše)</i>
Anonymizace údajů po ukončení doby jejich zpracování	<i>Jak se údaje anonymizují po ukončení doby, kdy má správce povinnost údaje uchovávat</i>

Má software certifikát souladu s GDPR

Má používaný software od výrobce certifikát či jiné závazné potvrzení o souladu s GDPR

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	1-5	
Ztráta dat	1-5	
Zranitelnost	1-5	
Vnější hrozba	1-5	

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší databáze s osobními daty a čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Poznámka

Záznam o činnostech zpracování – dokumenty – vzor

Název dokumentu	<i>Jméno dokumentu</i>
Popis dokumentu a účel dokumentu	<i>Popis obsahu dokumentu a k jakému účelu se používá</i>
Elektronická / Listinná / Obě verze	<i>O jakou verzi dokumentu se jedná</i>
Osobní údaje – základní	<i>Seznam základních osobních údajů, které jsou zpracovávány např. Jméno, příjmení, bydliště, datum narození, rodné číslo, e-mail, telefon</i>
Osobní údaje – ostatní	<i>Seznam ostatních osobních údajů, například národnost, věk, pohlaví</i>
Osobní údaje – citlivé	<i>Seznam osobních údajů – citlivé, například zdravotní dokumentace, finanční situace</i>
Povinnost zpracovávat údaje na základě právního nároku	<i>Na základě jakého předpisu, zákona, smlouvy organizace zpracovává osobní údaje</i>
Povinnost zpracovávat údaje po dobu podle právního nároku	<i>Po jak dlouhou dobu může organizace zpracovávat osobní údaje na základě výše uvedeného předpisu, zákona, smlouvy</i>
Evidence údajů nad právní rámec	<i>Zda se evidují osobní údaje nad právní rámec výše uvedený na základě souhlasu</i>
Bude vyžadován souhlas fyzické osoby (A/N)	<i>Bude vyžadován souhlas?</i>
Pohyb dokumentu v rámci organizace	<i>Jaká oddělení přicházejí do styku s dokumentem</i>
Předávání jiným zpracovatelům	<i>Zda a jak se dokument zasílá mimo organizaci, např. externí účetní</i>
Předávání jiným příjemcům	<i>Jakým příjemcům se dokumenty předávají např. OSSZ, ZP, správní orgány</i>
Předávání osobních údajů do jiných zemí	<i>Zda a jak se předávají osobní údaje do jiných zemí</i>
Způsob zabezpečení proti zneužití – elektronická verze	<i>Jak je dokument zajištěn proti neoprávněnému zneužití</i>
Způsob zabezpečení proti zneužití – listinná verze	<i>Zabezpečení dokumentu proti zneužití, zcizení, zničení</i>
Pracovní pozice s právem přístupu k osobním údajům	<i>Jaké pracovní pozice mají přístup k dokumentu</i>
Způsob archivace – elektronická verze	<i>Jak je dokument archivován</i>
Způsob archivace – listinná verze	<i>Způsob zajištění dokumentu pro archivaci</i>

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	1-5	
Ztráta dokumentu	1-5	
Zranitelnost	1-5	

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty a čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

--

Poznámka

--

Záznam o činnostech zpracování – informační systémy – Správa MŠ

Informační systém (jméno a výrobce)	Správa MŠ - Marek Michálek, Ke Kurtům 374, 14200 Praha 4
Popis software	Cloudová aplikace pro evidenci dětí
Modul	Školní matrika
Osobní údaje – základní	Jméno, příjmení, datum narození dítěte, bydliště, telefon, datum přijetí dítěte
Osobní údaje – ostatní	pohlaví, jazyk, příslušnost
Osobní údaje – citlivé	Rodné číslo, zákonní zástupci- jméno, příjmení, bydliště, kontakt, jména osob k vyzvednutí dítěte, datum a číslo jednacích rozsudků (rozvedení), pojišťovna dětí, zdravotní dokumentace, zaměstnanci - docházka, čerpání dovolené, evidence studijního volna
Povinnost zpracovávat údaje na základě právního nároku	Školský zákon 561/2004 Sb.
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ne
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	Word, Excel
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Zdravotní pojišťovna
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Zálohování dat a jejich zabezpečení	Denní záloha, větší zálohy každé 3 měsíce. Zabezpečení zajišťuje autor programu
Pracovní pozice s právem přístupu k osobním údajům	Zástupkyně ředitele, ředitelka, pedagogové (tisk, zapisování do matrik)
Anonymizace údajů po ukončení doby jejich zpracování	Ne – údaje se musí vymazat
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
------------	---------------	--------------

Důležitost údajů	4	Program obsahuje citlivé osobní údaje dětí
Ztráta dat	2	Program je dostatečně zabezpečen
Zranitelnost	2	Program je dostatečně zabezpečen
Vnější hrozba	2	Program je dostatečně zabezpečen

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší databáze s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Poznámka

--

Záznam o činnostech zpracování – informační systémy – VIS Plzeň

Informační systém (jméno a výrobce)	VIS Plzeň - Veřejná informační služba, spol. s r.o.
Popis software	Informační systém pro stravování dětí
Modul	Stravování
Osobní údaje – základní	Jméno, příjmení, datum narození, bydliště, číslo bankovního účtu, majitel účtu, telefon, email
Osobní údaje – ostatní	Variabilní symbol
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, Na základě plnění smlouvy
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ne
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	Excel, Word
Předávání údajů jiným zpracovatelům	Externí účetní Olga Vávrová Ičo:49984641, způsob předávání - osobně
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Zálohování dat a jejich zabezpečení	Záloha jednou týdně na disk v serveru
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí školní jídelny, ředitelka, pedagogové
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát souladu s GDPR	Ano

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivé osobní údaje

Ztráta dat	2	Program je dostatečně zabezpečen
Zranitelnost	2	Program je dostatečně zabezpečen
Vnější hrozba	2	Program je dostatečně zabezpečen

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší databáze s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme nastavit zálohování automaticky místo zálohy manuální.

Doporučujeme aktualizaci smluvního vztahu se zpracovatelem na základě nařízení GDPR a nastavení pravidel zabezpečení a archivace podle této směrnice u zpracovatele.

Poznámka

--

Záznam o činnostech zpracování – informační systémy – Mozilla Thunderbird

Informační systém (jméno a výrobce)	Mozilla Thunderbird – Mozilla Corporation
Popis software	Program pro elektronickou poštu
Modul	Elektronická pošta
Osobní údaje – základní	Jméno, příjmení, email
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Obsah sdělení, osobní data zaměstnanců
Povinnost zpracovávat údaje na základě právního nároku	Oprávněný zájem
Povinnost zpracovávat údaje po dobu podle právního nároku	Neomezeno
Evidence údajů nad právní rámec	Ne
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ne
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	Word, Excel, PDF
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, sporič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Zálohování dat a jejich zabezpečení	Záloha jednou týdně na disk v serveru
Pracovní pozice s právem přístupu k osobním údajům	Ředitelka
Anonymizace údajů po ukončení doby jejich zpracování	Ne
Má software certifikát souladu s GDPR	

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Emailový klient obsahuje osobní údaje zaměstnanců
Ztráta dat	2	Emailový klient je dostatečně zabezpečen

Zranitelnost	2	Emailový klient je dostatečně zabezpečen
Vnější hrozba	2	Emailový klient je dostatečně zabezpečen

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší databáze s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Mzdová a personální agenda

Název dokumentu	Pracovní smlouva, platový výměr, mzdový list, oznámení z rady města (přiznání odměny), dohody o provedení práce, náplň práce, evidenční list důchodového pojištění, osobní dotazník, dosažené vzdělání, výpis z evidence trestů, zdravotní průkaz, osobní dotazník, životopis, pověření vedení začínající učitelky, výplatní listky, rozúčtování mezd, hromadný příkaz, tabulka s měsíčním vyúčtováním, odměny, soupiska (přehled zaměstnanců, čerpání dovolené), přehled evidence pracovní doby v jednotlivých měsících, rozpisy služeb, plán dovolených, portfolio zaměstnance, doklady o průběžném vzdělávání, směrnice, řády, vnitřní pokyny, hmotná odpovědnost, BOZP
Popis dokumentu a účel dokumentu	Pro uzavření pracovně právního vztahu
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, rodinný stav, datum narození, rodné příjmení, místo narození, číslo občanského průkazu, telefon, číslo účtu, titul, číslo zaměstnance, počet stravenek, pohlaví
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Rodné číslo, mzda, trvání pracovního poměru, zdravotní pojišťovna, vyměřovací základ, datum počátku výdělečné činnosti, skupiny ŘP, záznam v rejstříku trestů, předchozí zaměstnavatel, jméno, příjmení, adresa, rodné číslo a zaměstnavatel, manžela/ky, jméno, příjmení dětí a data narození dětí, exekuce, vystudovaná škola a ročník studia, daňové zvýhodnění, druh školení, dlužná částka, podmínky oddlužení, průběh insolvence, druh uplatňovaných slev, data potřebná pro roční zúčtování daně, důchod, zdravotní stav, daňové slevy, vznik a zánik pracovního poměru, zdravotní pojištění, prohlášení k dani, údaje o mzdě a odvodech, druh lékařské prohlídky, druh práce, lékařský posudek, výše příspěvků, údaje o pojistné smlouvě, druh práce, povolené vycházky, informace o úrazu, důchod, údaje o mzdě a odvodech, příchody a odchody, dovolená, lékař, nemoc, číslo smlouvy pro ŽP A PP, výše příspěvku, srážky ze mzdy, evidence vydaných stravenek, podklad pro zasílání mezd, a obdobné dokumenty

Povinnost zpracovávat údaje na základě právního nároku	155/1995 Sb. Zákon o důchodovém pojištění, 235/2004 Zákon o dani z příjmů, 1/1992 Sb. Zákon o mzdě, 262/2006 Sb. Zákoník práce
Povinnost zpracovávat údaje po dobu podle právního nároku	30 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Ředitelka, zástupkyně – evidence pracovní doby a rozpisů služeb
Předávání jiným zpracovatelům	Externí účetní Olga Vávrová Ičo:49984641, způsob předávání - osobně
Předávání jiným příjemcům	Príslušné úřady
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Způsob zabezpečení proti zneužití – listinná verze	Uzamykatelná kancelář u ředitelky, zamykatelné skříně
Pracovní pozice s právem přístupu k osobním údajům	Ředitelka
Způsob archivace – elektronická verze	Po uplynutí doby právního nároku na evidenci jsou data smazána
Způsob archivace – listinná verze	Spisovný a skartační řád - archivní dokumenty předávány do spisovny (samostatná uzamykatelná místnost bez přístupu neoprávněných osob), po ukončení doby právního nároku jsou dokumenty skartovány

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	Dokumenty obsahují vysoce citlivá data zaměstnanců
Ztráta dokumentu	2	Dokumenty jsou dostatečně zabezpečeny
Zranitelnost	2	Dokumenty jsou dostatečně zabezpečeny

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme pořídit požární hlásič do archivu listinných dokumentů

Doporučujeme aktualizaci smluvního vztahu se zpracovatelem na základě nařízení GDPR a nastavení pravidel zabezpečení a archivace podle této směrnice u zpracovatele.
--

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Evidence dětí

Název dokumentu	Evidenční list dítěte, seznamy dětí na kulturní a sportovní akce, pověření pro předávání dětí, souhlasy, přehled o docházce dětí, diagnostiky dětí (hodnocení dítěte, schopnosti, tabulka s přehledem co dítě dosáhlo), portfolio dětí (práce dětí výtvarné, pracovní listy), evidence úrazů dětí
Popis dokumentu a účel dokumentu	Pro předškolní vzdělávání dítěte
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, datum narození dítěte, bydliště, telefon, datum přijetí dítěte
Osobní údaje – ostatní	Pohlaví, jazyk, příslušnost
Osobní údaje – citlivé	Rodné číslo, číslo jednací rozsudku (rozvedení)
Povinnost zpracovávat údaje na základě právního nároku	Školský zákon 561/2004 Sb.
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Osoba oprávněná k vyzvednutí dítěte
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Ředitelka, pedagogové
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Zdravotní pojišťovny, město Náchod
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Způsob zabezpečení proti zneužití – listinná verze	Uzamykatelná kancelář u ředitelky, zamykatelné skříň, budova zabezpečena zabezpečovacím zařízením
Pracovní pozice s právem přístupu k osobním údajům	Ředitelka, zástupkyně ředitelky
Způsob archivace – elektronická verze	Po uplynutí doby právního nároku na evidenci jsou data smazána
Způsob archivace – listinná verze	Samostatný archiv uzamčená místnost, uzamčené skříň, době právního nároku jsou dokumenty skartovány

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
------------	---------------	--------------

Důležitost údajů	4	Dokumenty obsahují citlivé osobní údaje dětí
Ztráta dokumentu	2	Dokumenty jsou dostatečně zabezpečeny
Zranitelnost	2	Dokumenty jsou dostatečně zabezpečeny

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme pořídit požární hlásič do archivu listinných dokumentů

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Stravování

Název dokumentu	Evidenční list přihláška, seznam plateb záloh, vyúčtování stravného, potvrzení o poskytnutí dávky pomoci nutné nouze, potvrzení od lékaře při úpravě stravování, potvrzení o úhradě školného (vystavuje vedoucí jídelny)
Popis dokumentu a účel dokumentu	Pro zajištění stravování dětí
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, datum narození, bydliště, číslo bankovního účtu, majitel účtu, telefon, email, doručovací adresa
Osobní údaje – ostatní	Variabilní symbol
Osobní údaje – citlivé	Registrační číslo
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, Na základě plnění smlouvy
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Vedoucí školní jídelny, ředitelka
Předávání jiným zpracovatelům	Externí účetní Olga Vávrová Ičo:49984641, způsob předávání - osobně
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Způsob zabezpečení proti zneužití – listinná verze	Uzamykatelná kancelář s přístupem pouze oprávněných osob, uzamykatelná skříň
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí školní jídelny, ředitelka
Způsob archivace – elektronická verze	Po uplynutí doby právního nároku na evidenci jsou data smazána
Způsob archivace – listinná verze	Samostatný archiv uzamčená místnost, uzamčené skříň, době právního nároku jsou dokumenty skartovány

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
------------	---------------	--------------

Důležitost údajů	3	Dokumenty neobsahují natolik citlivá data fyzických osob
Ztráta dokumentu	2	Dokumenty jsou dostatečně zabezpečeny
Zranitelnost	2	Dokumenty jsou dostatečně zabezpečeny

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme pořídit požární hlásič do archivu listinných dokumentů
Doporučujeme aktualizaci smluvního vztahu se zpracovatelem na základě nařízení GDPR a nastavení pravidel zabezpečení a archivace podle této směrnice u zpracovatele.

Poznámka

--

Záznam o činnostech zpracování - dokumenty - Účetnictví

Název dokumentu	Dodavatelské faktury, pokladní doklady, bankovní výpisy, revize, inventarizace, měsíční hlášení hospodaření skladu školní jídelny, vyřazovací protokoly, rozvaha, obratová předvaha, účetní doklad majetek, objednávky
Popis dokumentu a účel dokumentu	Pro vedení účetnictví
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, adresa, IČ, DIČ, email, telefon
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Vedoucí školní jídelny, ředitelka
Předávání jiným zpracovatelům	Externí účetní Olga Vávrová Ičo:49984641, způsob předávání - osobně
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Počítač zabezpečen heslem - velká a malá písmena a číslice v délce minimálně 6 znaků, spořič obrazovky po 10 minutách nečinnosti, zamčená kancelář
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty uloženy v uzamykatelné kanceláři, uzamykatelná skříň
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí školní jídelny, ředitelka
Způsob archivace – elektronická verze	Po uplynutí doby právního nároku na evidenci jsou data smazána
Způsob archivace – listinná verze	Samostatný archiv uzamčená místnost, uzamčené skříň, době právního nároku jsou dokumenty skartovány

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty neobsahují citlivé údaje fyzických osob

Ztráta dokumentu	2	Dokumenty jsou dostatečně zabezpečeny
Zranitelnost	2	Dokumenty jsou dostatečně zabezpečeny

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme pořídit požární hlásič do archivu listinných dokumentů
Doporučujeme aktualizaci smluvního vztahu se zpracovatelem na základě nařízení GDPR a nastavení pravidel zabezpečení a archivace podle této směrnice u zpracovatele.

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Kniha pošty

Název dokumentu	Kniha pošty
Popis dokumentu a účel dokumentu	Pro evidenci pošty
Elektronická/Listinná/Obě verze	L
Osobní údaje – základní	Jméno, příjmení, adresa
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	Oprávněný zájem
Povinnost zpracovávat údaje po dobu podle právního nároku	Neomezeno
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Ne
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Nevede se
Způsob zabezpečení proti zneužití – listinná verze	Uzamykatelná skříň v uzamykatelné kanceláři
Pracovní pozice s právem přístupu k osobním údajům	Ředitelka, zástupkyně ředitelky
Způsob archivace – elektronická verze	Nevede se
Způsob archivace – listinná verze	Dokument předán do spisovny (samostatná uzamykatelná místnost bez přístupu neoprávněných osob)

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Dokument neobsahuje citlivá data fyzických osob
Ztráta dokumentu	2	Dokument je dostatečně zabezpečen
Zranitelnost	2	Dokument je dostatečně zabezpečen

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší dokument (soubor) s osobními daty, čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Doporučujeme pořídit požární hlásič do archivu listinných dokumentů

Poznámka

--

Záznam o činnostech zpracování – informační systémy – Kamerový systém

Informační systém (jméno a výrobce)	Kamerový systém , Aremic s.r.o. Náchod
Popis softwaru	<i>On-line kamera umístěná při vstupu do budovy MŠ, na zahradě a v ředitelně</i>
Účel zpracování	<i>zvýšení bezpečnosti osob (napadení, loupež, krádež, jiná fyzická újma) = ochrana života a zdraví osob,</i> <i>prevence mimořádných událostí,</i> <i>získávání důkazního materiálu pro příslušné odpovědné orgány (soudy a Policie ČR v případě trestných činů, obecní úřady v případě řešení přestupků),</i> <i>získávání materiálu pro řešení pojistných událostí (s věcně příslušnou pojišťovnou).</i> <i>zvýšení ochrany majetku (krádež, vloupání, vandalismus)</i>
Osobní údaje – základní	<i>Záznam obrazu</i>
Osobní údaje – ostatní	<i>Ne</i>
Osobní údaje – citlivé	<i>Ne</i>
Povinnost zpracovávat údaje na základě právního nároku	<i>Oprávněný zájem</i>
Povinnost zpracovávat údaje po dobu podle právního nároku	<i>Uchovávání záznamu na datovém disku s dobou 7 dní od data záznamu</i>
Evidence údajů nad právní rámec	<i>Ne</i>
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	<i>Ne</i>
Předávání údajů do jiných systémů v rámci organizace – způsob	<i>Ne</i>
Možnosti exportů dat ze systému	<i>Ne</i>
Předávání údajů jiným zpracovatelům	<i>Ne</i>
Předávání údajů jiným příjemcům	<i>Orgány činné v trestním řízení v případě mimořádné události,</i> <i>Orgány činné v přestupkovém řízení v případě mimořádné události,</i> <i>Pojišťovny v případě řešení pojistné události,</i> <i>Subjekty údajů v případě jejich požadavku (jen záběry, kde se vyskytují tyto osoby, ostatní části jsou anonymizované).</i>

	<i>Zpracovatel (pokud správce má najatého zpracovatele, který provádí některé operace zpracování osobních údajů za správce) var. pro kamery v režimu online: Osobní údaje nejsou předávány jiným příjemcům.</i>
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	<i>Datový disk umístěn v uzamčené datové skříni v uzamykatelné místnosti v ředitelně organizace</i>
Zálohování dat a jejich zabezpečení	<i>Záznam je uchováván na datovém disku umístěném v datové skříni v ředitelně organizace</i>
Pracovní pozice s právem přístupu k osobním údajům	Ředitelka
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát o souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Mohou být zaznamenána citlivá osobní data
Ztráta dat	2	Mohou být zaznamenána citlivá osobní data
Zranitelnost	2	Kamerový systém vzhledem k citlivosti údajů zabezpečen přiměřeně
Vnější hrozba	2	Kamerový systém vzhledem k citlivosti údajů zabezpečen přiměřeně

Čím vyšší riziko, tím vyšší známka. Čím rozsáhlejší databáze s osobními daty a čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Poznámka

S. Prezenční listina pracovníků, kteří jsou seznámeni se směrnicí k GDPR a zákonu č. 110/2019

Jméno a příjmení	Pracovní pozice v organizaci	Podpis

Výše uvedení pracovníci organizace potvrzují svým podpisem, že byli seznámeni s pravidly pro ochranu a nakládání s osobními daty podle směrnice GDPR pro příspěvkovou organizaci. Pravidlům uvedených v této směrnici rozumí a budou se jimi při vykonávání své práce řídit.

V Náchodě dne 01.05.2025