



Směrnice GDPR pro příspěvkovou organizaci

**Střední škola automobilní Ústí
nad Orlicí
IČO: 00529842**



... Máme řešení i pro Vaši společnost

www.softbit.cz

Obsah

Účel	3
K čemu slouží	3
Pro koho je určena	3
Stanovení zásad	3
Zákonnosti	3
Podmínky pro udělení souhlasu	4
Podmínky použitelné pro souhlas dítěte v souvislosti se službami informační společnosti	4
Korektnost a transparentnost	4
Účelové omezení	5
Minimalizace údajů	5
Přesnost	5
Omezení uložení	6
Integrita a důvěrnost	6
Odpovědnost	6
Způsob ochrany osobních údajů	6
Způsoby anonymizace po ukončení zpracování osobních údajů	8
Způsoby pseudonymizace osobních údajů	9
Způsoby předávání osobních údajů v rámci společnosti	9
Způsoby předávání osobních údajů jiným zpracovatelům	9
Způsoby předávání osobních údajů dalším příjemcům	10
Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím	10
Zpracování osobních údajů za účelem cíleného marketingu	10
Právo subjektu údajů na přístup k osobním datům	11
Zajištění práva přenositelnosti subjektu údajů	12
Právo fyzické osoby na opravu	12
Právo fyzické osoby na výmaz	12
Právo na omezení zpracování	13
Hlášení bezpečnostních incidentů	13
Stanovení Pověřence pro ochranu osobních údajů (DPO)	14
Školení pracovníků, kteří přicházejí do styku s osobními údaji	15
Oddělení ve společnosti, která se řídí směrnici	16
Prezenční listina zaměstnanců, kteří jsou seznámeni se směrnici k GDPR	16
Vysvětlivky některých pojmů	17
Udělení souhlasu s poskytnutím osobních údajů - vzor	18
Zrušení uděleného souhlasu k poskytnutí osobních údajů - vzor	19
Karta evidovaných osobních údajů v organizaci o subjektu údajů / fyzické osobě – vzor	20
Varianta zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem	21
Záznamy o činnostech	23



Účel

Účelem vnitropodnikové 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.

K čemu slouží

Směrnice slouží ke správnému nakládání s osobními údaji subjektu údajů podle nařízení 2016/679 Evropského parlamentu a Rady (EU), dále jen nařízení GDPR.

Pro koho je určena

Pro všechny pracovníky organizace, kteří přicházejí do styku s osobními údaji subjektu údajů.

Stanovení zásad (podle článku 5 nařízení GDPR)

Organizace se řídí jednotlivými zásadami, které stanovuje nařízení GDPR. Směrnice obsahuje jednotlivé dokumenty, soubory a databáze, ve kterých jsou evidovány osobní údaje.

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
- Oprávněného zájmu
- Na základě plnění či uzavření 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 tabulek software a dokumentů používaných ve společnosti.

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)

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 společnosti (podle článku 8 nařízení GDPR)

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 fyzická osoba udělila souhlas se zpracováním osobních údajů k jednomu nebo více konkrétním účelům v souvislosti s nabídkou služeb informační společnosti přímo dítěti, je zpracování osobních údajů dítěte zákonné, je-li dítě ve věku nejméně 16 let.

Je-li dítě mladší 16 let, organizace zajistí pro zákonnost takového zpracování osobních údajů souhlas osoby, která vykonává rodičovskou povinnost k dítěti.

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 ty osobní údaje, 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.

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.

Způsoby ochrany osobních údajů

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

Písenná podoba – dokumenty obsahující osobní údaje – v produkčním prostředí

Dokumenty obsahující osobní data, jsou v uzamykatelných 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.

Písenná 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 zabezpečovacím systémem.
Po ukončení platnosti dokumentů nebo doby, po kterou dokumenty mohou být v organizaci uloženy, jsou tyto dokumenty skartovány. Skartaci dokumentů provádí pověřený pracovník (zaměstnanec organizace).
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 uložišti(serveru) společnosti, 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 malá a velká písmena a číslice v délce minimálně 8 znaků. Přístupy do systémů mají pouze oprávnění pracovníci, kteří mohou zpracovávat osobní data subjektu údajů.
Přístupy do informačních systémů jsou pravidelně obměňovány v časovém intervalu 1 roku. Je zajištěno, aby se hesla neopakovala.
Každý počítač je jistěn uživatelským heslem obsahujícím malá a velká písmena a číslice v délce minimálně 8 znaků.
Při vzdálení se od PC je pracovník povinen zamknout tento klávesovou zkratkou Windows klávesa + L.
Uživatelská hesla do osobních počítačů a pro přístup na společné uložště jsou obměňována jednou za 1 rok. Je zajištěno, aby se hesla neopakovala.
Při nečinnosti pracovníka na osobním PC v délce větší jak 10 min. je tento automaticky zamykán uživatelským heslem.
Pracovníci, kteří přicházejí do styku s osobními daty, 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.
V případech, kdy informační systém neobsahuje funkci evidence exportů, jsou pracovníci povinni před provedením exportu požádat o povolení pověřenou osobu, zpravidla správce IT.

Osobní údaje uložené v mobilních telefonech pracovníků organizace jsou chráněny proti zcizení, zničení nebo zneužití nastaveným PIN kódem při přihlášení do mobilního telefonu, vstupním kódem při odemykání. Uložení kontaktů s osobními údaji je synchronizováno pomocí služby cloud.

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 proti vnějším hrozbám je chráněn bránou Firewall OS Debian. Na PC stanicích i datovém serveru (využívá-li platformu Windows) je instalován pravidelně aktualizovaný antivirový program Avast Endpoint Protection Suite.

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

Soubory a databáze s osobními daty jsou pravidelně 1x denně 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. Historické zálohy dat jsou v organizaci uchovávány po dobu 1 měsíce.

Zabezpečené uložení pro produkční zálohy elektronických dat obsahujících mimo jiné i osobní údaje subjektu údajů se nachází technicky na datovém serveru organizace, vzdáleném uložení v cloudu, na externím zařízení připojením k datovému serveru organizace.

K zálohám produkčních databází a souborů má přístup pouze k tomu pověřená osoba, zpravidla správce IT a jeho zástupce. Správce IT rovněž provádí výmaz historických záloh po době jejich plánovaného uchovávání.

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 jiným zpracovatelem.

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.

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 na konci této směrnice.
Anonymizaci 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 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.

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 formou pseudonymizace.

Způsoby předávání osobních údajů v rámci společnosti

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

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

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 je uveden na konci této směrnice.

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 formou zabezpečené zprávy pomocí datových schránek.
Zasílání dokumentů a souborů, které obsahují osobní data, je prováděno ostatním zpracovatelům pomocí e-mailové korespondence, kdy je příloha 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 a pod). 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.

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 formou zabezpečené zprávy pomocí datových schránek.

Zasílání dokumentů a souborů, které obsahují osobní data, je prováděno ostatním příjemcům pomocí e-mailové korespondence, kdy je příloha 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 a pod). 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.

Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (podle článku 44 nařízení GDPR)

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

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 zpracování.

Právo subjektu údajů na přístup k osobním údajům (podle článku 15 nařízení *GDPR*)

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 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 pracovník organizace si 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 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.

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

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.

Zajištění práva přenositelnosti subjektu údajů *(podle článku 20 nařízení GDPR)*

Organizace zajišťuje právo subjektu údajů na přenositelnost osobních dat k jiným správcům. V případě, že subjekt údajů požádá organizaci o předání osobních dat pro jejich převedení jiný správce, 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)*

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 osoba 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.

Právo fyzické osoby na výmaz *(podle článku 17 nařízení GDPR)*

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)

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.
--

Hlášení bezpečnostních incidentů (podle článku 33 nařízení GDPR)

V případě, že dojde v organizaci k porušení bezpečnosti zpracovávaných osobních dat, které může mít za následek poškození práv a svobod osob subjektu údajů, ředitel(ka) 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.

Stanovení Pověřence pro ochranu osobních údajů (DPO) (podle článku 37 nařízení GDPR)

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

Jméno	Tomáš Urban
Organizace	Softbit software s.r.o.
Telefon	603 449 244
Email	tomas.urban@softbit.cz

Zástupce pověřence pro ochranu osobních údajů

Jméno	Ing. Jeroným Holý
Organizace	Softbit software s.r.o.
Telefon	736 159 010
Email	jeronym.holy@softbit.cz

Jméno	Tomáš Holý
Organizace	Softbit software s.r.o.
Telefon	776 570 423
Email	tomas.holy@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 provádí zejména:

Poskytování informací a poradenství správci a dalším zpracovatelům a zaměstnancům, kteří provádějí zpracování osobních údajů o jejich povinnostech podle tohoto nařízení GDPR.

Monitoruje provádění ochrany osobních údajů fyzických osob v organizaci v souladu s nařízením GDPR.

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.

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 a směrnici k ochraně osobních údajů.

Pracovníci, kteří přicházejí do styku s osobními údaji, zachovávají plnou mlčenlivost ve vztahu k jiným osobám a společnostem, které nemají žádný právní nárok tyto informace požadovat.

Oddělení v organizaci, která se řídí směrnicí

V organizaci se řídí nařízením k GDPR o ochraně osobních údajů fyzických osob a směrnicí k tomuto nařízení tato oddělení:

Ředitel(ka) organizace
Ekonomické a účetní oddělení
Mzdová účtárna a personální oddělení
Pedagogičtí pracovníci
Pracovníci autoškoly
Pracovníci STK a SME
Sklad
Mechanici a opraváři motorových vozidel

Prezenční listina pracovníků, kteří jsou seznámeni se směrnicí k GDPR

Prezenční listina pracovníků je přílohou této směrnice.

V Ústí nad Orlicí dne 23. 5. 2018

Podpis ředitele organizace:	
-----------------------------	--

Podpis pověřence pro ochranu osobních dat:	
--	--

Vysvětlivky některých pojmů

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

Subjekt údajů – fyzická osoba, která je předmětem ochrany osobních údajů.

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

Správce – organizace, která provádí zpracování osobních údajů, vlastník směrnice GDPR.

Zpracovatel – organizace, která provádí zpracování osobních údajů pro správce.

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.

Udělení souhlasu s poskytnutím osobních údajů

Správce

Název organizace	
IČ :	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.

Správce

Subjekt údajů / Fyzická osoba

.....

.....

(čitelný podpis, datum)

(čitelný podpis, datum)

Zrušení uděleného souhlasu k poskytnutí osobních údajů

Správce

Název organizace	
IČ :	Dič :

Subjekt údajů /Fyzická osoba

Jméno a příjmení	
Bydliště	
Doklad totožnosti	

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

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

Udělený souhlas ruším pro tyto účely:

Správce

Subjekt údajů / Fyzická osoba

.....

(čitelný podpis, datum)

.....

(čitelný podpis, datum)

Karta evidovaných osobních údajů v organizaci o subjektu údajů / fyzické osobě

Správce

Název organizace	
IČ :	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 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

.....

.....

Podpis

Podpis

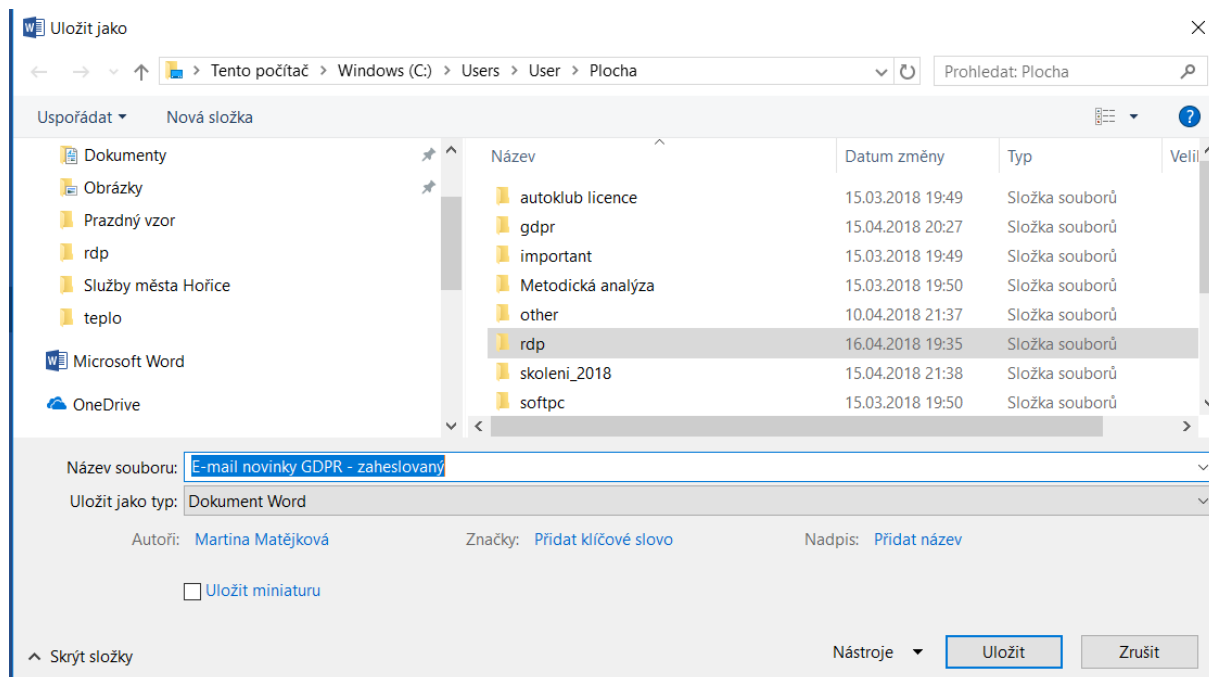
Varianta zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem

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.

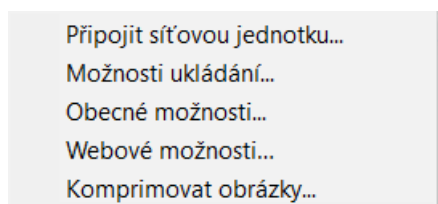
Tuto funkci podporují například kancelářské programy MS Word nebo MS Excel, ale i jiné.

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

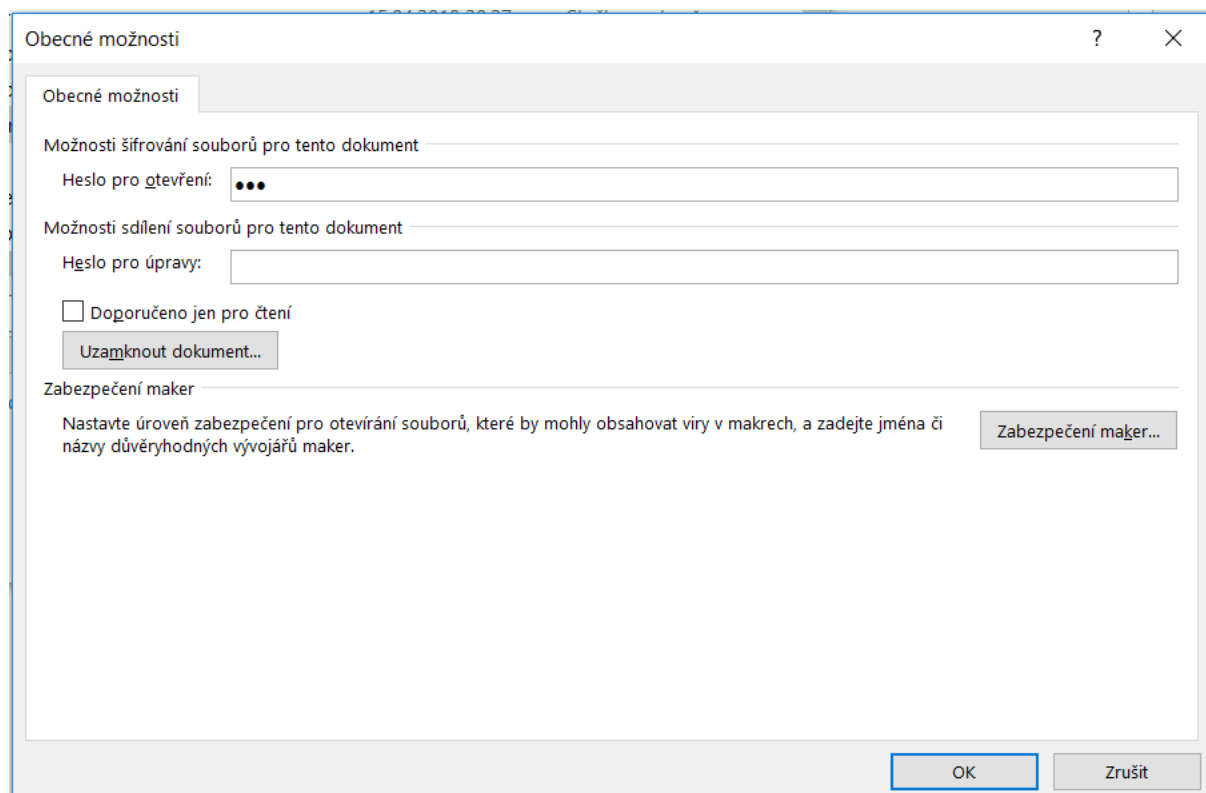
1. Vytvořený soubor uložíme přes funkci „Uložit jako“. Při ukládání zadáme název souboru s odlišným názvem než je původní, který si ponecháme ve svém počítači (tento zpravidla nebudeme doplňovat heslem pro jeho otevření).
2. Zvolíme nabídku „Nástroje“ a zde vybereme funkci „Obecné možnosti“.
3. V údajích „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“

Záznam o činnostech zpracování – informační systémy - Ginis

Informační systém (jméno a výrobce)	Ginis - Gordic a.s.
Popis software	Systém správy dokumentů
Modul	GWASSD
Osobní údaje – základní	Jméno, příjmení, adresa, IČ, DIČ
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	499/2004 Sb. Zákon o archivnictví a spisové službě
Povinnost zpracovávat údaje po dobu podle právního nároku	45 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, pdf
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Gordic a.s., 47903783, technický zásah, společnost hostuje a spravuje databázi
Předávání údajů jiným příjemcům	Pardubický kraj
Předávání osobních údajů do jiných zemí	Pardubický kraj
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut, šifrovaný přenos
Zálohování dat a jejich zabezpečení	Zálohování programu zajišťuje Pardubický kraj
Pracovní pozice s právem přístupu k osobním údajům	Podatelna (sekretariát) a zástup v případě nepřítomnosti
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program obsahuje pouze základní 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

Poznámka

--

Záznam o činnostech zpracování – informační systémy – **Vema HR**

Informační systém (jméno a výrobce)	VEMA HR, Vema a.s.
Popis software	Informační systé, pro řízení lidských zdrojů
Modul	Mzdy, Personalistika, Evidenční listy důchodového pojištění, Registr nemocenského pojištění
Osobní údaje – základní	Jméno, příjmení, bydliště, rodinný stav, datum narození, rodné příjmení, místo narození, číslo občanského průkazu, telefon, číslo účtu, titul, číslo zaměstnance
Osobní údaje – ostatní	Národnost, pohlaví, občanství
Osobní údaje – citlivé	Druh práce, plat, rodné číslo, exekuce, zdravotní způsobilost, rodné číslo, půjčky, úvěry, počet odebrané stravy v jídelně
Povinnost zpracovávat údaje na základě právního nároku	Zák. č. 262/2006 zákoník práce, Zák. č. 99/1963 občanský soudní řád, exekuční řád, Zák. č. 435/2004 o zaměstnanosti, Zák. č. 251/2005 o inspekci práce, Zák. č. 2/1991 o kolektivním vyjednávání, Zák. č. 89/2013 občanský zákoník, Zák. č. 500/2004 správní řád, Zák. č. 586/1992 o daních z příjmů, Zák. č. 187/2006 o nemocenském pojištění, Zák. č. 582/1991 o organizaci a provádění soc. zabezpečení, Zák. č. 99/1963 občanský soudní řád, 592/1992 Sb. zákon o pojistném na veřejné zdravotní pojištění, 563/1991 Sb., zákon o účetnictví
Povinnost zpracovávat údaje po dobu podle právního nároku	45 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	Export do Excel, Word, pdf, xml
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Vema a.s., 26226511, připojení přes vzdálenou plochu - technický zásah
Předávání údajů jiným příjemcům	Portál ČSSZ, Zdravotní pojišťovny ČR, Finanční správa
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut

Zálohování dat a jejich zabezpečení	Zálohuje se denně na server v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Všichni s PC (každý může mít jiná práva)
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	Program obsahuje vysoce citlivá data mzdové a personální agendy
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 - **Certis**

Informační systém (jméno a výrobce)	Certis - CERMAT
Popis software	Maturitní zkouška, přijímačky
Modul	Klasifikace, volba předmětů
Osobní údaje – základní	Jméno, příjmení, adresa, datum narození, bydliště
Osobní údaje – ostatní	Státní příslušnost, pohlaví
Osobní údaje – citlivé	Dysfunkce, rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	561/2004 Sb. Školský zákon
Povinnost zpracovávat údaje po dobu podle právního nároku	45 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	Ano, excel, word
Předávání údajů jiným zpracovatelům	CERMAT, 72029455
Servisní přístup k software	CERMAT, 72029455, vzdálená plocha (technické problémy), napojení do databáze IS Certis od společnosti CERMAT (řádný provoz)
Předávání údajů jiným příjemcům	CERMAT
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Uzamčený a nepřístupný PC označený jako "DDT", přihlášení do systému CERMATU pod heslem, veškerou správu včetně zabezpečení PC vzdáleně zajišťuje CERMAT.
Zálohování dat a jejich zabezpečení	Zálohování celého počítače zajišťuje CERMAT
Pracovní pozice s právem přístupu k osobním údajům	Pedagogové, admin. pracovníci pověřeni, diferencovaně
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	3	Program obsahuje citlivá data fyzických osob
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 - Databáze - kurzy

Informační systém (jméno a výrobce)	Databáze - kurzy - Martin Vojtěch
Popis software	Informační systém na správu osobních údajů řidičů a lektorů
Modul	Jmenný seznam řidičů, adresář, pravidelné školení, lektoři
Osobní údaje – základní	Jméno a příjmení, datum narození, bydliště, telefon, email, číslo ŘP a PP
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	Seznam účastníků pravidelného školení podle § 48 odst. 2 a 5, Seznam účastníků pravidelného školení dle Zákona č.247/2000 Sb. ve znění Zákona č.374/2007 Sb.
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Rodné číslo
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ano
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	Ano, excel, word
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Data se dále nepředávají, běh zajišťuje správce IS školy SŠA
Předávání údajů jiným příjemcům	ORP
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Zálohování dat a jejich zabezpečení	NAS server pod heslem, šifrovaný archiv - 8 znaků, zálohováno dle potřeby
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí školícího střediska, asistentka, IT správce
Anonymizace údajů po ukončení doby jejich zpracování	Ne
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivá data fyzických osob
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 - **Stravné**

Informační systém (jméno a výrobce)	Stravné – VIS Plzeň
Popis software	Program slouží k evidenci strávníků školní jídelny a bezhotovostních plateb
Modul	Strava, Sklad
Osobní údaje – základní	Jméno, příjmení, bydliště, obor studia, ročník, email, číslo účtu, číslo karty, evidenční číslo, telefon, datum narození
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Dieta
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, § 119 školského zákona
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu studia + 5 měsíců
Evidence údajů nad právní rámec	Email, telefon
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ano
Předávání údajů do jiných systémů v rámci společnosti – způsob	SQL Ekonom – export dat
Možnosti exportů dat ze systému	Word, Excel
Předávání údajů jiným zpracovatelům	VIS Plzeň
Servisní přístup k software	VIS Plzeň, 45330344, po telefonické domluvě vzdálená plocha nebo osobní návštěva technika
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Zálohování dat a jejich zabezpečení	Data uložena na serveru, který je denně zálohován na NAS
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí kuchyně, ekonomický úsek
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje až na výjimky citlivá data fyzických osob
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

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

Záznam o činnostech zpracování – informační systémy – SQL Ekonom

Informační systém (jméno a výrobce)	SQL Ekonom – SOFTbit Software s.r.o.
Popis software	Informační systém pro vedení účetnictví, skladu, prodeje, fakturace, adresáře, pošty a banky
Modul	Došlé faktury, vydané faktury, banka, pokladna, sklady, adresář, majetek, účetnictví, zakázky
Osobní údaje – základní	Jméno, příjmení, adresa, IČ, telefon, číslo bankovního účtu, osobní číslo, datum narození
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Dluh, insolvence, exekuce
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, 235/2004 Sb. Zákon o DPH, 16/1993 Sb. Zákon o dani silniční, 89/2012 Sb. Občanský zákoník
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, PDF
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Softbit Software s.r.o., 274 73 716, přístup přes vzdálenou plochu, v případě problémů si spol. stáhne kopii celé databáze
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Zálohování dat a jejich zabezpečení	Data ze serveru se zálohují denně přes server na NAS v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí pracovníci, pracovníci EÚ, pracovníci zpracovávající skladovou agendu, pokladny, majetek a zakázky
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	4	Program obsahuje citlivá data fyzických osob
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 – **Emise 2013**

Informační systém (jméno a výrobce)	Emise 2013 – Dekra a.s.
Popis software	IS pro stanice měření emisí
Modul	X
Osobní údaje – základní	Jméno, adresa, spz (+ další info o vozidle typu VIN apod.), ič, dič
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	302/2001 Sb. Vyhláška Ministerstva dopravy a spojů o technických prohlídkách a měření emisí vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 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	SQL Ekonom – export dat
Možnosti exportů dat ze systému	Zálohová SQL soubor
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Dekra a.s., 49240188, po tlf. Domluvě vzdálená plocha případně osobní návštěva technika
Předávání údajů jiným příjemcům	Ministerstvo dopravy
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Zálohování dat a jejich zabezpečení	Záloha databáze denní na NAS server pod heslem
Pracovní pozice s právem přístupu k osobním údajům	Pracovník ME
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Program obsahuje citlivá data fyzických osob
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 – **Kipas**

Informační systém (jméno a výrobce)	Kipas - VDO
Popis software	Kalibrace tachografů
Modul	X
Osobní údaje – základní	Jméno, adresa, spz (+ další info o vozidle typu VIN apod.), ič, dič
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	505/1990 Sb. Zákon o metrologii, nařízení rady ES 561/2006
Povinnost zpracovávat údaje po dobu podle právního nároku	5 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	SQL Ekonom – export dat
Možnosti exportů dat ze systému	Word, Excel
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Mechanika Děčín, 00556157, telefon nebo vzdálená plocha (zatím nevyužito...)
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut, program se spouští s pomocí čipové karty, vše v samostatné uzamčené místnosti
Zálohování dat a jejich zabezpečení	1x za týden se zálohují na optický disk zašifrovaná data z tachografů (klíč je pro nás neznámý)
Pracovní pozice s právem přístupu k osobním údajům	Oprávněný pracovník
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Program obsahuje citlivá data fyzických osob
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 – CIS plus

Informační systém (jméno a výrobce)	CIS plus – Dekra a.s.
Popis software	IS pro stanice STK
Modul	X
Osobní údaje – základní	Jméno, adresa, spz (+ další info o vozidle typu VIN apod.), ič, dič
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	302/2001 Sb. Vyhláška Ministerstva dopravy a spojů o technických prohlídkách a měření emisí vozidel, 56/2001 Sb. Zákon o podmínkách provozu vozidel na pozemních komunikacích
Povinnost zpracovávat údaje po dobu podle právního nároku	5 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	SQL Ekonom – export dat
Možnosti exportů dat ze systému	Databáze ve formě SQL pro zálohy
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Dekra a.s., 49240188, po tlf. Domluvě vzdálená plocha případně osobní návštěva technika
Předávání údajů jiným příjemcům	Ministerstvo dopravy
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut, povinnost měnit heslo každé 3 měsíce
Zálohování dat a jejich zabezpečení	Denní záloha databáze na NAS server pod heslem - 10 zn.
Pracovní pozice s právem přístupu k osobním údajům	Pracovník ME
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ano

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivá data fyzických osob

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 -

Viper

Informační systém (jméno a výrobce)	Viper – Dekra a.s.
Popis software	IS pro dovozy a přestavby vozidel
Modul	X
Osobní údaje – základní	Jméno, adresa, spz (+ další info o vozidle typu VIN apod.), ič, dič
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	56/2001 Sb. Zákon o podmínkách provozu vozidel na pozemních komunikacích
Povinnost zpracovávat údaje po dobu podle právního nároku	5 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	SQL Ekonom – export dat
Možnosti exportů dat ze systému	Tiskové sestavy
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Dekra a.s., 49240188, po tlf. Domluvě vzdálená plocha případně osobní návštěva technika
Předávání údajů jiným příjemcům	Městský úřad obor dopravy
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut, povinnost měnit heslo každé 3 měsíce
Zálohování dat a jejich zabezpečení	Denní záloha databáze na NAS server pod heslem - 10 zn.
Pracovní pozice s právem přístupu k osobním údajům	Pověření pracovníci
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ano

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program obsahuje pouze základní 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

Poznámka

--

Záznam o činnostech zpracování – informační systémy - **Bakaláři**

Informační systém (jméno a výrobce)	Bakaláři - BAKALÁŘI Software, s.r.o.
Popis software	Program pro evidenci žáků základní školy, doklady o přijímání žáků o průběhu a ukončení vzdělávání
Modul	Bakaláři, Evidence, Úvazky, Rozvrh hodin, Suplování, Třídní kniha, Zápis známek
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, telefon, email
Osobní údaje – ostatní	Národnost, státní příslušnost, pohlaví
Osobní údaje – citlivé	Zdravotní stav, kázeňská opatření, tresty
Povinnost zpracovávat údaje na základě právního nároku	§ 28 odst. 1 písm. b) školského zákona
Povinnost zpracovávat údaje po dobu podle právního nároku	45 let
Evidence údajů nad právní rámec	Kontakt na zákonné zástupce
Bude vyžadován pro zpracování souhlas fyzické osoby (A/N)	Ano
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	.doc, .xls, .pdf a další
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Bakaláři software s.r.o., 27483045, vzdálená plocha po tlf. Domluvě
Předávání údajů jiným příjemcům	MŠMT
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut, automatické odpojení od systému po 10 minutách nečinnosti
Zálohování dat a jejich zabezpečení	Denní záloha na NAS umístěný v uzamykatelné místnosti
Pracovní pozice s právem přístupu k osobním údajům	Pedagogové, administrativní pracovníci
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Program obsahuje citlivé osobní údaje žáků

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 - Čerpačka

Informační systém (jméno a výrobce)	Čerpačka - Styles Znojmo
Popis software	Software k čerpací stanici
Modul	PHW
Osobní údaje – základní	Jméno, příjmení, adresa
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	Na základě uzavření či plnění smlouvy
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu platnosti smlouvy
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	Ne
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Styles znojmo, 46967362, vzdálená plocha vč. Zkopírování dtb., návštěva technika
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do programu obsahující velká a malá písmena a numerický znak v délce 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu 2 minut, autologon pro případ výpadku elektřiny
Zálohování dat a jejich zabezpečení	Denní záloha na NAS umístěný v uzamykatelné místnosti
Pracovní pozice s právem přístupu k osobním údajům	Vedoucí dílen, zaměstnanec ek. Úseku, pracovníci pověřeni správou programu
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivé osobní údaje žáků
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 - Elektronická pošta

Informační systém (jméno a výrobce)	Microsoft Outlook – Microsoft Corporation, Mozilla Thunderbird – Mozilla Corporation, Windows Live Mail – Microsoft Corporation
Popis software	Elektronická pošta
Modul	Elektronická pošta
Osobní údaje – základní	Jméno, příjmení, email
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 pro zpracování souhlas fyzické osoby (A/N)	Ne
Předávání údajů do jiných systémů v rámci společnosti – způsob	Ne
Možnosti exportů dat ze systému	Jakákoliv příloha
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	OG Soft s.r.o., 25108565, vzdálená plocha, administrace serverů, osobní návštěvy technika
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu 2 minut
Zálohování dat a jejich zabezpečení	V rámci serveru, denní záloha, zaheslováno, vlastní VLAN pro zálohu serveru
Pracovní pozice s právem přístupu k osobním údajům	Každý uživatel
Anonymizace údajů po ukončení doby jejich zpracování	Neprovádí se
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivé osobní údaje fyzických osob
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 - **GACC**

Informační systém (jméno a výrobce)	GACC - Job Abasus Pro
Popis software	Čipové otevírání dveří
Modul	Elektronická pošta
Osobní údaje – základní	Jméno, příjmení, email
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	Není evidováno
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	Databáze výrobci v případě technických problémů
Předávání údajů jiným zpracovatelům	Ne
Servisní přístup k software	Epimo, 62061283, osobní návštěva technika
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu 10 minut, nutno znát IP - běží ve virtuálním stroji, uživatelský login - 8 znaků
Zálohování dat a jejich zabezpečení	Záloha na serveru denní celého virtuálního stroje na uzamčený NAS
Pracovní pozice s právem přístupu k osobním údajům	Správce IT
Anonymizace údajů po ukončení doby jejich zpracování	Manuální výmaz
Má software certifikát souladu s GDPR	Ne

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Program neobsahuje citlivé osobní údaje fyzických osob
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 - dokumenty –**Akce pořádané školou**

Název dokumentu	Soutěže, exkurze, olympiády, sportovní kurzy, brigády, praxe žáků
Popis dokumentu a účel dokumentu	Přehled zúčastněných pro organizátory i naši školu (účast, absence, zodpovědnost za žáky)
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, číslo občanského průkazu
Osobní údaje – ostatní	Věk
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	Oprávněný zájem, ostatní na základě udělení souhlasu
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu využitelnosti dokumentu nebo po dobu platnosti
Evidence údajů nad právní rámec	Kontakty na zákonné zástupce, zdravotní problémy, další dle konkrétního souhlasu
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Třídní učitelé, učitelé
Předávání jiným zpracovatelům	Jiná škola, zařízení (podle charakteru akce)
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Pověřený pracovník má u sebe
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, zástupce ředitele, třídní učitelé, učitelé, účetní
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Dokumenty neobsahují citlivé osobní údaje
Ztráta dokumentu	3	Dokumenty má u sebe v listinné podobě pověřený pracovník
Zranitelnost	3	Dokumenty má u sebe v listinné podobě pověřený pracovník

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

Poznámka

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

Záznam o činnostech zpracování - dokumenty – Ekonomická agenda

Název dokumentu	Objednávky, smlouvy, doklad o předběžné kontrole, došlé faktury, podklady k DPH, silniční dani, dani z příjmu PO, bankovní výpisy, pokladní doklady, vydané faktury, pohledávky a upomínky k VF, podklady k soudnímu vymáhání pohledávek, PAP, platby např. za stravné, ubytování, kurzy a další služby pro žáky, zaměstnance a cizí osoby, žádosti o dotace pro žáky a zaměstnance, rozhodnutí o poskytnutí dotací
Popis dokumentu a účel dokumentu	Objednávání materiálu, zboží a služeb, zpracování došlých faktur, data k zúčtování daní, hotovostní a bezhotovostní platební styk, fakturace odběratelům, odsouhlasení a vymáhání pohledávek, zpracování účetních závěrek, evidence úhrad např. za stravné, ubytování, kurzy a další služby pro žáky, zaměstnance a cizí osoby, přidělení dotací žákům a zaměstnancům na základě vyhlášení dotačních programů
Elektronická/Listinná/Obě verze	Obě
Osobní údaje – základní	jméno, příjmení, bydliště, datum narození, č. OP, telefon, č. účtu, titul, osobní číslo zaměstnance a žáka, IČO, DIČ
Osobní údaje – ostatní	Národnost
Osobní údaje – citlivé	Rodné číslo, mzda, exekuce, druh školení, výše pohledávky, data potřebná pro roční zúčtování daně, výše přidělené dotace
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, 235/2004 Sb. Zákon o dani z příjmu, 16/1993 Sb. Zákon o dani silniční, 89/2012 Sb. Občanský zákoník, 218/2000 Sb. Zákon o rozpočtových pravidlech
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	Ředitel, vedoucí a pověření pracovníci

Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Finanční úřad, Krajský úřad, MŠMT, Úřad práce
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do programu obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti, která je chráněna kamerovým systémem
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, vedoucí a pověření pracovníci
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Dokumenty neobsahují citlivé osobní 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

Poznámka

--

Záznam o činnostech zpracování - dokumenty –**Mzdy a personalistika**

Název dokumentu	Pracovní smlouvy, platové výměry, dohody o pracovní činnosti, dohody o provedení práce, ukončení pracovního poměru, zdravotní prohlídky, evidence pracovní doby a obdobné
Popis dokumentu a účel dokumentu	Vznik a ukončení pracovního poměru, vstupní a periodické zdravotní prohlídky, plnění pracovních povinností
Elektronická/Listinná/Obě verze	Obě
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, rodné číslo, email, telefon
Osobní údaje – ostatní	Věk, pohlaví
Osobní údaje – citlivé	Výše mzdy, exekuce, srážky ze mzdy, dosažené vzdělání, zdravotní stav, fotografie
Povinnost zpracovávat údaje na základě právního nároku	561/2004 Sb., školský zákon, 286/200 Sb., o ochraně veřejného zdraví, 499/2004 Sb., zákon o archivnictví a spis. službě, Spisový a skartační řád školy, 563/2004 Sb., zákon o pedagogických pracovnících, 564/2006 Sb., o pl. poměrech zaměstnanců ve veřejných službách a správě
Povinnost zpracovávat údaje po dobu podle právního nároku	30 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Mzdová účetní, ředitel školy
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	ČSSZ, Zdravotní pojišťovny ČR, Finanční úřad, Úřad práce, Česká pojišťovna, Respect, insurance brokers
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do programu obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti, která je chráněna kamerovým systémem

Pracovní pozice s právem přístupu k osobním údajům	Ředitel, zástupce ředitele, mzdová účetní, účetní
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	Dokumenty obsahují vysoce citlivé osobní 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

--

Poznámka

--

Záznam o činnostech zpracování - dokumenty –**Stravování a ubytování**

Název dokumentu	Osobní spis žáka, Přihláška do DM, Pedagogický deník, přihlášky ke stravování
Popis dokumentu a účel dokumentu	Evidence ubytovaných, jejich chování, plány jednotlivých skupin, evidence styku se zákonnými zástupci, spolupráce s třídním učitelem a mistrem, evidence strážníků
Elektronická/Listinná/Obě verze	L
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, místo narození, číslo bankovního účtu, obor, třída
Osobní údaje – ostatní	Věk, pohlaví
Osobní údaje – citlivé	Výchovná opatření, evidence prospěchu, rodné číslo, zdravotní pojišťovna
Povinnost zpracovávat údaje na základě právního nároku	Vyhláška č. 107/2005 Sb. o školním stravování, Vyhláška č. 255/2007 Sb. o FKSP, Vyhláška č. 34/1991 Sb. o hospodářské činnosti škol
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	Skupinový vychovatel, ředitel, vedoucí kuchyně
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Školní inspekce
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Nevede se
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Vychovatelé, vedoucí domova, ředitel, třídní učitel, mistr, vedoucí kuchyně
Způsob archivace – elektronická verze	Nevede se
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní 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 zálohovat tato data na server organizace i mimo budovu organizace, např. na cloud.

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Kostní dřeň

Název dokumentu	Seznam žáků
Popis dokumentu a účel dokumentu	přehled zúčastněných pro naši školu (účast žáků, absence, zodpovědnost za žáky)
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, číslo občanského průkazu
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo, pojišťovna
Povinnost zpracovávat údaje na základě právního nároku	Na základě souhlasu
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu platnosti souhlasu
Evidence údajů nad právní rámec	Veškeré údaje
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Ředitel, zástupce ředitele, třídní učitelé, učitelé
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Zdravotnické zařízení
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Pověřený pracovník má u sebe
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, zástupce ředitele, třídní učitelé, učitelé
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Listinné dokumenty jsou uloženy ve skříni v uzamykatelné kanceláři

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje žáků
Ztráta dokumentu	3	Dokumenty má u sebe v listinné podobě pověřený pracovník
Zranitelnost	3	Dokumenty má u sebe v listinné podobě pověřený pracovník

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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Zkoušky – **MZ, ZZ, opravné, doplňkové**

Název dokumentu	Seznam přihlášených žáků
Popis dokumentu a účel dokumentu	Přehled žáků, volba zkoušky, termín
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, předmět
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	561/2004 Sb. Školský zákon
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Třídní učitelé, učitelé, administrativní pracovníci
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Pověřený pracovník má u sebe
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, zástupce ředitele, třídní učitelé, učitelé, administrativní pracovníci
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Dokumenty obsahují pouze základní osobní údaje fyzických osob
Ztráta dokumentu	3	Dokumenty má u sebe v listinné podobě pověřený pracovník
Zranitelnost	3	Dokumenty má u sebe v listinné podobě pověřený pracovník

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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Doplnkové vzdělání – Školení emisních techniků a svářečských pracovníků

Název dokumentu	Přihlášky na školení - papírová verze, databáze školenců, třídní knihy, doklad o absolvování školení, cena školení, návratky rodičů, zdravotní způsobilost potvrzená lékařem
Popis dokumentu a účel dokumentu	Přihlášení na školení, evidence přihlášených osob, evidence jejich osobních dat, které jsou vedeny pro účely identifikace a komunikace a kontroly příslušnému, kontrolnímu orgánu doklad o absolvování školení, doklad o osobním převzetí potvrzení o absolvování školení, evidence nepřítomnosti na výuce, evidence vyučujících lektorů, zdravotní způsobilost účastníků
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, telefon, email, série a číslo řidičského průkazu
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	Oprávněný zájem, 56/2001 Sb. Zákon o podmínkách provozu vozidel na pozemních komunikacích
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Vedoucí střediska 531 - vzdělávání dospělých, asistentka vedoucího střediska, účetní, lektori, energetický technik,
Předávání jiným zpracovatelům	DOM - ZO 13, s.r.o., IČ: 25261908
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, vedoucí střediska 531 - vzdělávání dospělých, asistentka vedoucího střediska
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze

Způsob archivace – listinná verze	Dokumenty jsou archivovány v uzamčené místnosti, uzamykatelná skříň, skartace dle Spisového a skartačního řádu školy (5 let)
-----------------------------------	--

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

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

Záznam o činnostech zpracování - dokumenty – Doplnkové vzdělání – manipulační vozíky a elektroškolení - SŠA Jantač středisko 530

Název dokumentu	Přihlášky na školení - papírová verze, databáze školenců, třídní knihy, doklad o absolvování školení, cena školení, návratky rodičů, zdravotní způsobilost potvrzená lékařem
Popis dokumentu a účel dokumentu	Přihlášení na školení, evidence přihlášených osob, evidence jejich osobních dat, které jsou vedeny pro účely identifikace a komunikace a kontroly příslušnému, kontrolnímu orgánu doklad o absolvování školení, doklad o osobním převzetí potvrzení o absolvování školení, evidence nepřítomnosti na výuce, evidence vyučujících lektorů, zdravotní způsobilost účastníků
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, telefon, email, série a číslo řidičského průkazu
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Rodné číslo, zdravotní způsobilost
Povinnost zpracovávat údaje na základě právního nároku	247/2000 Sb. Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel, 347/2007 Sb. Zákon, kterým se mění zákon č. 120/2001 Sb. Zákon o soudních exekutorech a exekuční činnosti (exekuční řád)
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Ředitel, vedoucí střediska 530 - vzdělávání dospělých, asistentka vedoucího střediska, účetní, lektori, energetický technik
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	ORP, krajský úřad, městský úřad
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, vedoucí střediska 531 - vzdělávání dospělých, asistentka vedoucího střediska
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na

	uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Dokumenty jsou archivovány v uzamčené místnosti, uzamykatelná skříň, skartace dle Spisového a skartačního řádu školy (5 let)

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Doplňkové vzdělání – Profesní školení pro řidiče SŠA Jantač středisko

530

Název dokumentu	Přihlášky na školení - papírová i elektronická verze, databáze řidičů, třídní knihy, doklad o absolvování školení, cena školení
Popis dokumentu a účel dokumentu	Přihlášení na školení, evidence přihlášených osob, evidence jejich osobních dat, které jsou vedeny pro účely identifikace a komunikace a kontroly příslušnému, kontrolnímu orgánu doklad o absolvování školení, doklad o osobním převzetí potvrzení o absolvování školení, evidence nepřítomnosti na výuce, evidence vyučujících lektorů
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, telefon, email, série a číslo řidičského průkazu
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	247/2000 Sb. Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel, 347/2007 Sb. Zákon, kterým se mění zákon č. 120/2001 Sb. Zákon o soudních exekutorech a exekuční činnosti (exekuční řád)
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Ředitel, vedoucí střediska 530 - vzdělávání dospělých, asistentka vedoucího střediska, účetní, lektori
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	ORP, Krajský úřad, Městský úřad, Ministerstvo dopravy ČR
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, vedoucí střediska 531 - vzdělávání dospělých, asistentka vedoucího střediska
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na

	uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Dokumenty jsou archivovány v uzamčené místnosti, uzamykatelná skříň, skartace dle Spisového a skartačního řádu školy (5 let)

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

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

Záznam o činnostech zpracování - dokumenty – Doplnkové vzdělání – KJP SŠA Jantač středisko 530

Název dokumentu	Předběžné přihlášky na studium, závazné přihlášky na studium, smlouvy o studiu, el. verze smlouvy o studiu, papírová verze - kopie jejich vysvědčení z učiliště či základní školy, u žen ještě kopie oddacího listu, doklad o změně jména, přihlášky ke zkouškám a přihlášky k maturitě, vypracované testy - závěrečné zkoušky, opravné testy - opravné závěrečné zkoušky, databáze studentů, osvědčení, maturitní vysvědčení, protokoly o předání maturitního vysvědčení, omluvenky z konání zkoušek
Popis dokumentu a účel dokumentu	Předběžné přihlášení na studium, závazné přihlášení na studium, potřebný smluvní vztah, doložení předchozího vzdělání + průkaznost změny jména, evidence přihlášení ke zkouškám a k maturitním zkouškám, zjišťování jejich znalostí, evidence jejich osobních dat, které jsou vedeny pro účely identifikace a komunikace, osvědčení a maturitní vysvědčení - doklad o ukončeném vzdělání na naší škole, doklad o osobním převzetí maturitního vysvědčení studentem, omluvenky - evidence nepřítomnosti na zkouškách
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, rodné příjmení, místo narození, telefon, email
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Dosažené vzdělání
Povinnost zpracovávat údaje na základě právního nároku	561/2004 Sb. Školský zákon
Povinnost zpracovávat údaje po dobu podle právního nároku	45 let
Evidence údajů nad právní rámec	Kontakt – telefon, email
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Ředitel, vedoucí střediska 530 - vzdělávání dospělých, asistentka vedoucího střediska, účetní, administrativní správce přihlášek k maturitě, vrátná
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	CERMAT
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce

	minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Dokumenty jsou uloženy v uzamčené skříni v uzamčené místnosti
Pracovní pozice s právem přístupu k osobním údajům	Ředitel, vedoucí střediska 531 - vzdělávání dospělých, asistentka vedoucího střediska
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

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

Záznam o činnostech zpracování - dokumenty – Protokol STK

Název dokumentu	Protokol o technické prohlídce, protokol před reg. Vozidla, na žádost zákazníka, před schválením tech způsobilosti, prohlídka po sil. Kontrole, opakované prohlídky, prohlídka ADR (nebezpečné náklady)
Popis dokumentu a účel dokumentu	Prokázání technické způsobilosti auta
Elektronická/Listinná/Obě verze	L
Osobní údaje – základní	Jméno, příjmení, adresa, SPZ, číslo TP, IČ, DIČ
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	302/2001 Sb. Vyhláška Ministerstva dopravy a spojů o technických prohlídkách a měření emisí vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	STK, ME, tachografy
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	kontrolní orgány (KÚ Pk, MDČR)
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Nevede se
Způsob zabezpečení proti zneužití – listinná verze	Archivace pouze záznamník závad - dokumenty se po vytištění uzamknou v šuplíku v uzamykatelné kanceláři a jednou za týden jsou přesunuty do "archivu" na Dukle, který je elektronicky zabezpečen
Pracovní pozice s právem přístupu k osobním údajům	Pověření pracovníci
Způsob archivace – elektronická verze	Nevede se
Způsob archivace – listinná verze	Uzamčené dokumenty v centrálním archivu Dukla, elektronické zabezpečení senzorem pohybu

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Protokol emise

Název dokumentu	Protokol o technické prohlídce, protokol před reg. Vozidla, na žádost zákazníka, před schválením tech způsobilosti, prohlídka po sil. Kontrole, opakované prohlídky, prohlídka ADR (nebezpečné náklady)
Popis dokumentu a účel dokumentu	Prokázání technické způsobilosti auta
Elektronická/Listinná/Obě verze	L
Osobní údaje – základní	Jméno, příjmení, adresa, SPZ, číslo TP, IČ, DIČ
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo
Povinnost zpracovávat údaje na základě právního nároku	302/2001 Sb. Vyhláška Ministerstva dopravy a spojů o technických prohlídkách a měření emisí vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	STK, ME, tachografy
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	kontrolní orgány (KÚ Pk, MDČR)
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Nevede se
Způsob zabezpečení proti zneužití – listinná verze	Protokoly se po vytištění uzamknou v šuplíku v uzamykatelné kanceláři a jednou za týden jsou přesunuty do "archivu" na Dukle, který je elektronicky zabezpečen
Pracovní pozice s právem přístupu k osobním údajům	Pověření pracovníci
Způsob archivace – elektronická verze	Nevede se
Způsob archivace – listinná verze	Uzamčené dokumenty v centrálním archivu Dukla, elektronické zabezpečení senzorem pohybu

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
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

Poznámka

--

Záznam o činnostech zpracování - dokumenty - Autoškola

Název dokumentu	Přihláška do autoškoly
Popis dokumentu a účel dokumentu	Evidence přihlášek
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, datum narození, místo narození, Telefon, bydliště, PSČ, doklad totožnosti, typ řidičského průkazu
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Zdravotní stav, rodné číslo, úřad s rozšířenou působností
Povinnost zpracovávat údaje na základě právního nároku	247/2000 Sb. Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	AŠ, sekretariát
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Dopravní inspektorát
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	V šuplíku v místnosti zabezpečené alarmem s přístupem pouze oprávněných osob
Pracovní pozice s právem přístupu k osobním údajům	Pověřený pracovník autoškoly
Způsob archivace – elektronická verze	Denní zálohování celého systému na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje
Ztráta dokumentu	2	Dokumenty jsou dostatečně zabezpečeny
Zranitelnost	2	Dokumenty jsou dostatečně zabezpečeny

Nápravná opatření pro snížení rizik

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Třídní knihy

Název dokumentu	Třídní knihy
Popis dokumentu a účel dokumentu	Třídní knihy
Elektronická/Listinná/Obě verze	L
Osobní údaje – základní	Jméno, příjmení, datum narození, telefon, bydliště, PSČ, typ řidičského průkazu
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	247/2000 Sb. Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Kontakt na zákonné zástupce
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	Zaměstnanci autoškoly
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	Dokumenty jsou uloženy v zamykatelné místnosti (sborovna AŠ), do rukou ji dostanou pouze oprávnění zaměstnanci pro výuku pro danou hodinu
Pracovní pozice s právem přístupu k osobním údajům	Oprávnění zaměstnanci pro výuku
Způsob archivace – elektronická verze	Nevede se
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle skartačního řádu

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	Dokumenty obsahují pouze základní osobní údaje
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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Evidence **autoškoly**

Název dokumentu	Evidenční kniha, hlášenka kurzu, hlášenka ke zkouškám
Popis dokumentu a účel dokumentu	Evidence autoškoly, pro potřeby úřadu - dopravní inspektorát
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, datum narození, místo narození, doklad totožnosti, telefon, bydliště, PSČ, typ a číslo řidičského průkazu, evidenční číslo
Osobní údaje – ostatní	Občanství
Osobní údaje – citlivé	Zdravotní stav, rodné číslo, výsledek závěrečné zkoušky, platby, úřad s rozšířenou působností
Povinnost zpracovávat údaje na základě právního nároku	247/2000 Sb. Zákon o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Pověření pracovníci AŠ
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	MěÚ - dopravní inspektorát
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Po naskenování a odeslání smazáno
Způsob zabezpečení proti zneužití – listinná verze	V šuplíku v místnosti zabezpečené alarmem
Pracovní pozice s právem přístupu k osobním údajům	Pověření pracovníci AŠ
Způsob archivace – elektronická verze	Bez archivace, dokumenty jsou po zpracování vytisknuty a smazány z datového úložiště
Způsob archivace – listinná verze	Samostatná místnost (archiv) zabezpečená elektronickým zabezpečovacím systémem, skartace dle Spisového a skartačního řádu školy

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	Dokumenty obsahují vysoce citlivé osobní 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

Poznámka

--

Záznam o činnostech zpracování - dokumenty – Lékařské prohlídky

Název dokumentu	Tisk formuláře na lékařské prohlídky (excel s makry)
Popis dokumentu a účel dokumentu	Lékařské prohlídky
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, bydliště, datum narození, titul, číslo zaměstnance, číslo řidičského průkazu
Osobní údaje – ostatní	Věk, pohlaví
Osobní údaje – citlivé	Druh práce, jiná oprávnění k výkonu práce
Povinnost zpracovávat údaje na základě právního nároku	262/2006 Sb. Zákoník práce, 48/1997 Sb. Zákon o veřejném zdravotním pojištění
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu platnosti dle zařazení zaměstnance, po dobu studia u žáka
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	Všichni s PC (každý může mít jiná práva)
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	Heslo do počítače obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, heslo do sítě obsahující velká a malá písmena a numerický znak v délce minimálně 8 znaků, spořič obrazovky v intervalu maximálně 10 minut
Způsob zabezpečení proti zneužití – listinná verze	Pověřený pracovník má u sebe
Pracovní pozice s právem přístupu k osobním údajům	Všichni s PC (každý může mít jiná práva)
Způsob archivace – elektronická verze	Denní zálohování xls souboru na uzamčený server, který je zálohován na uzamčený NAS, po uplynutí doby právního nároku výmaz z databáze
Způsob archivace – listinná verze	Dokumenty jsou skartovány po době využitelnosti

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	Dokumenty obsahují citlivé osobní údaje fyzických osob
Ztráta dokumentu	3	Dokumenty má u sebe v listinné podobě pověřený pracovník

Zranitelnost	3	Dokumenty má u sebe v listinné podobě pověřený pracovník
--------------	---	--

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

Poznámka

--