Domov odpočinku ve stáří JUSTYNKA, Komenského náměstí 212, Hronov, 549 31

Směrnice

Č. SD / 5 / 2011

Pravidla pro zpracování, vedení a evidenci dokumentace uživatelů (podle GDPR)

Platnost: 1.5.2018

Účinnost: 25.5.2018

Vyhotovil: Ing. Jitka Ansorgová, Irena Ducháčová, Bc. Ilona Šrejberová

Schválil: Ing. Jitka Ansorgová

Vlastník dokumentu: SP

Znalost dokumentu: Ř, VZSP, SP

Úložiště dokumentu: 004

Počet stran: 61
Výtisk: devátý
Konec platnosti: do příští aktualizace

Obsah

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 idenfitikovat 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.

Písemná podoba – dokumenty obsahující osobní údaje – v produkčním prostředí

Dokumenty obsahující osobní data, jsou v kancelářích uzavřeny v uzamykatelných skříních.
Do kanceláří a uzamykatelných skříní má přístup pouze odpovědná osoba seznámená s ochranou osobních údajů.
Dokumenty obsahující osobní data nejsou poskytovány žádné další osobě, která nemá právo na nahlížení k těmto datům ani nemá právo s nimi dále pracovat.
Pracovníci jsou seznámeni s tím, že listinné dokumenty obsahující osobní data nesmí ponechávat dostupné v kancelářích bez dozoru odpovědné osoby.

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

Archivní dokumenty obsahující osobní data jsou uzavřeny v samostatné místnosti (spisovně) organizace, která je zajištěna proti vniknutí osobám, které k tomu nemají oprávnění; spisovna je zajištěna před poškozením v něm uložených dokumentům proti požáru a dalším vnějším vlivům, které mohou znehodnotit takto uložené dokumenty.
Po ukončení platnosti dokumentů nebo doby, po kterou dokumenty mohou být v organizaci uloženy, jsou tyto dokumenty skartovány na základě Spisového a skartačního řádu Sd/16/2008.
Je vedena evidence všech dokumentů, které jsou ve spisovně uloženy a to i těch, které byly skartovány či předány do státního archivu.

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

Elektronické soubory s osobními daty jsou uloženy na zabezpečeném společném uložišti umístěném na datovém serveru, kam mají přístup jen oprávnění pracovníci organizace. Elektronické soubory s osobními daty jsou v maximálně možné míře zajištěny proti zcizení, zničení, vnějším hrozbám a jinému neoprávněnému zpracování. Datový server i stanice chráněny antivirovým systémem. Datový server pro blokování vnějšího přístupu je zajištěn bránou Firewall.
Přístupy do informačních systémů obsahujících osobní data jsou zajištěny hesly obsahujícími minimálně tři alfanumerické znaky a tři číslice v délce 6 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 jištěn uživatelským heslem obsahujícím minimálně 8 znaků (kombinace malých, velkých písmen, čísel a speciální znak).
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 uložiště 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 funkcionalita zajišťuje zpětnou kontrolu o tom, kdo, kdy a co exportoval a k jakému účelu.
Osobní údaje uložené v mobilních telefonech pracovníků organizace jsou chráněny proti zcizení, zničení nebo zneužití nastaveným PIN kódem při přihlášení do mobilního telefonu, nebo 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 seznámení s tím, že bez svolení vedení organizace nebudou tato data za žádných okolností ukládat, duplikovat či zálohovat do jiných než předem schválených umístění.

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

Soubory a databáze s osobními daty jsou pravidelně 1x denně v nočních hodinách zálohovány na externí datový disk. Tyto zálohy dat jsou využívány pro případ obnovy po havárii produkčních dat. Po obnově dat z těchto záloh jsou nejprve osobní data aktualizována na poslední známý stav a teprve po tomto kroku jsou data uvolněna k dalšímu zpracování.
Zabezpečené uložiště pro produkční zálohy elektronických dat obsahujících mimo jiné i osobní údaje subjektu údajů se nachází technicky na datovém serveru organizace, 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.
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 každý 1 měsíc. Archivní zálohy dat jsou v organizaci uchovávány po dobu jednoho měsíce.
V případě, že se provádí záloha produkčních dat do uložiště, které není pod správou organizace, má zajištěno pod smlouvou garanci zajištění bezpečnosti uložených dat jiným zpracovatelem.
Zabezpečené uložiště 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 uložiště 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.
Anonymizace písemných dokumentů je provedena formou nevratného přemazání osobních údajů subjektu, které vede k tomu, že daná osoba není zpětně identifikovatelná.

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 uložišti organizace, kam mají přístup pouze pracovníci oprávněni 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 neoprávněna 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 pomoc 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 neoprávněna 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 pomoc 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:

Po obdržení žádosti organizace prověří totožnost žadatele a to, zda fyzická osoba má právo požadovat výpis osobních údajů.
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.
Subjekt údajů má právo výslednou zprávu obdržet do 30 dní od data zaslání a ověření žádosti.
Výsledná zpráva je pro subjekt údajů bezplatná.

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 použitá 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 správcům, potom:

Organizace ověří totožnost žadatele a zákonnost této žádosti.
V přiměřené lhůtě, která odpovídá časové náročnosti takovéhoto 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.

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 osobě požaduje opravit, odpovídají skutečnosti.
Po ověření správce provede změnu osobních údajů dle nových skutečností ve všech evidencích, které zmíněné osobní údaje obsahují.

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	Tomáš Holý
Organizace	Softbit software s.r.o.
Telefon	776 570 423
Email	tomas.holy@softbit.cz

Jméno	Ing. Jeroným Holý
Organizace	Softbit software s.r.o.
Telefon	736 159 010
Email	jeronym.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 vnitropodnikovou 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 ve společnosti, která se řídí směrnicí

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

Ředitel(ka) společnosti
Ekonomické a účetní oddělení
Mzdová účtárna a personální oddělení
Sociální pracovnice
Zdravotní sestra

Prezenční listina zaměstnanců, kteří jsou seznámení se směrnicí k GDPR

Jméno a příjmení	Pracovní pozice ve společnosti	Podpis

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

V Hronově. dne 16.5.2018

Podpis ředitele (jednatele) společnosti :

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, zaznamenávaní, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použit, 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 účely :

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

.....

(čitelný podpis,datum)

Subjekt údajů / Fyzická osoba

.....

(čitelný podpis,datum)

Domov odpočinku ve stáří JUSTYNKA,

Komenského náměstí 212, Hronov, 549 31, IČ 62726226

Písemný souhlas s úschovou občanského průkazu

JMÉNO A PŘÍJMENÍ KLIENTA : ….....

DATUM NAROZENÍ : ….....

(v případě, že je shodnost jmen klientů)

Souhlasím níže svým podpisem s využitím nabídky úschovy svého občanského průkazu v Domově odpočinku ve stáří JUSTYNKA Hronov, a to na bezpečném místě v uzamykatelné skříni kanceláře účetní.

Byl/a, jsem poučen/a, že:

- toto své rozhodnutí mohu kdykoli změnit a ponechat si občanský průkaz u sebe
- že přístup k tomuto osobnímu dokladu má v Domově pouze účetní, sociální pracovník, vrchní sestra, zdravotní sestra a ředitel
- že s ním bude nakládáno s mým vědomím pouze za účelem nezbytně nutným v rámci plnohodnotného poskytování sociální služby
- úschova občanského průkazu bude pouze po dobu mého souhlasu
- občanský průkaz nebude Domovem odpočinku ve stáří JUSTYNKA Hronov předáván třetím stranám bez mého vědomí

V Hronově dne ……

……

Podpis klienta/klientky

Domov odpočinku ve stáří JUSTYNKA,

Komenského náměstí 212, Hronov, 549 31, IČ 62726226

Písemný souhlas s úschovou průkazu pojištěnce zdravotní pojišťovny

JMÉNO A PŘÍJMENÍ KLIENTA : ….....

DATUM NAROZENÍ : ….....

(v případě, že je shodnost jmen klientů)

Souhlasím níže svým podpisem s využitím nabídky úschovy svého průkazu pojištěnce zdravotní pojišťovny v Domově odpočinku ve stáří JUSTYNKA Hronov, a to na bezpečném místě v uzamykatelné skříni na sesterně Domova.

Byl/a, jsem poučen/a, že:

- toto své rozhodnutí mohu kdykoli změnit a ponechat si průkaz pojištěnce u sebe
- že přístup k tomuto osobnímu dokladu má v Domově pouze vrchní sestra a zdravotní sestra
- že s ním bude nakládáno s mým vědomím pouze za účelem nezbytně nutným v rámci plnohodnotného poskytování zdravotních služeb
- průkaz pojištěnce nebude Domovem odpočinku ve stáří JUSTYNKA Hronov předáván třetím stranám bez mého vědomí

V Hronově dne …… ……

Podpis klienta/klientky

Domov odpočinku ve stáří JUSTYNKA,

Komenského náměstí 212, Hronov, 549 31, IČ 62726226

SOUHLAS S NAHLÍŽENÍM DO ZDRAV. DOKUMENTACE (SZP + LÉKAŘ DO JUSTYNKA)

SOUHLAS S POSKYTNUTÍM ZDRAVOTNÍCH SLUŽEB

(zdravotních výkonů)

JMÉNO A PŘÍJMENÍ KLIENTA : ….....

DATUM NAROZENÍ : ….....

Souhlasím s nahlížením do mé zdravotní dokumentace, s poskytováním zdravotních služeb a s prováděním zdravotních výkonů k diagnostickým a léčebným účelům dle ordinace lékaře a dle mého aktuálního zdravotního stavu a při akutní potřebě ošetření.

Správce se zavazuje nepředávat výše uvedené informace třetím stranám. Souhlas správci poskytuji do doby jeho odvolání.

Jsem si vědom(a) svého práva zrušit kdykoli 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 mého svobodného rozhodnutí a není podmínkou pro zajištění ostatních služeb ze strany organizace k subjektu údajů.

VLASTNORUČNÍ PODPIS KLIENTA : ….....

PODPIS SVĚDKŮ, POKUD KLIENT NENÍ SCHOPEN

SE VLASTNORUČNĚ PODEPSAT: .....

PODPIS ZDRAVOTNICKÉHO PRACOVNÍKA : ….....

V HRONOVĚ DNE : ….....

Domov odpočinku ve stáří JUSTYNKA,

Komenského náměstí 212, Hronov, 549 31, IČ 62726226

SOUHLAS S POSKYTOVÁNÍM INFORMACÍ

JMÉNO A PŘÍJMENÍ KLIENTA : ….....

DATUM NAROZENÍ : ….....

SOUHLASÍM, aby informace o mém zdravotním stavu byly poskytovány

ÚSTNĚ, PÍSEMNĚ, TELEFONICKY níže jmenovanému :

JMÉNO A PŘÍJMENÍ : ….....

ADRESA : ….....

VZTAH KE KLIENTOVI : ….....

JMÉNO A PŘÍJMENÍ : ….....

ADRESA : ….....

VZTAH KE KLIENTOVI : ….....

Dále souhlasím, zda jmenovaný

MŮŽE - NEMŮŽE nahlížet do zdravotní dokumentace, zda

MŮŽE - NEMŮŽE pořizovat výpisky nebo kopie těchto dokumentů, zda

MÁ - NEMÁ právo vyslovit souhlas nebo nesouhlas s poskytnutím zdravotních služeb klientovi, pokud tak nemůže učinit sám klient.

NESOUHLASÍM, aby informace o mém zdravotním stavu byly komukoliv poskytovány.

Správce se zavazuje nepředávat výše uvedené informace třetím stranám. Souhlas správci poskytuji do doby jeho odvolání.

Jsem si vědom(a) svého práva zrušit kdykoli 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 mého svobodného rozhodnutí a není podmínkou pro zajištění ostatních služeb ze strany organizace k subjektu údajů.

VLASTNORUČNÍ PODPIS KLIENTA : ….....

PODPIS SVĚDKŮ, POKUD KLIENT NENÍ SCHOPEN

SE VLASTNORUČNĚ PODEPSAT : ….....

PODPIS ZDRAVOTNICKÉHO PRACOVNÍKA : ….....

V HRONOVĚ DNE : ….....

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

…….

(čitelný podpis,datum)

Subjekt údajů / Fyzická osoba

……..

(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

Domov odpočinku ve stáří JUSTYNKA,

Komenského náměstí 212, Hronov, 549 31, IČ 62726226

JMÉNO A PŘÍJMENÍ KLIENTA : ….....

DATUM NAROZENÍ : ….....

Já, klient **Domova odpočinku ve stáří JUSTYNKA Hronov** (dále jen domov), dávám svůj souhlas ke shromažďování, zpracovávání a evidenci osobních údajů a osobních citlivých údajů o mé osobě ve smyslu Nařízení Evropského parlamentu a Rady (EU) číslo 2016/679 a směrnice organizace ke GDPR. Svůj souhlas poskytuji pouze pro účely:

1. **Písemný souhlas s fotografováním a jiným obrazovým (zvukovým) záznamem mé osoby**

Souhlasím níže svým podpisem s fotografováním a jiným obrazovým a zvukovým záznamem, na kterém bude moje osoba za účelem veřejné prezentace Domova odpočinku ve stáří JUSTYNKA na webových stránkách organizace, Facebooku, tiskových materiálech a jiných obdobných. Jsem seznámen(a) s tím, že mohou být tyto obrazové záznamy poskytnuty regionálním tiskovým periodikům za účelem propagace domova.

Tento souhlas platí po dobu mého pobytu v domově a byl(a) jsem poučen(a) o svém právu tento souhlas kdykoliv bez udání důvodu písemně odvolat. Správce osobních údajů je povinen zrušení tohoto souhlasu k účelům, ke kterým byl udělen, bezodkladně provést.
Odvoláním souhlasu však není dotčena zákonnost zpracování osobních údajů v organizaci po dobu platnosti souhlasu.
Souhlas je vyjádřením mého svobodného rozhodnutí a není podmínkou pro zajištění ostatních služeb ze strany domova.

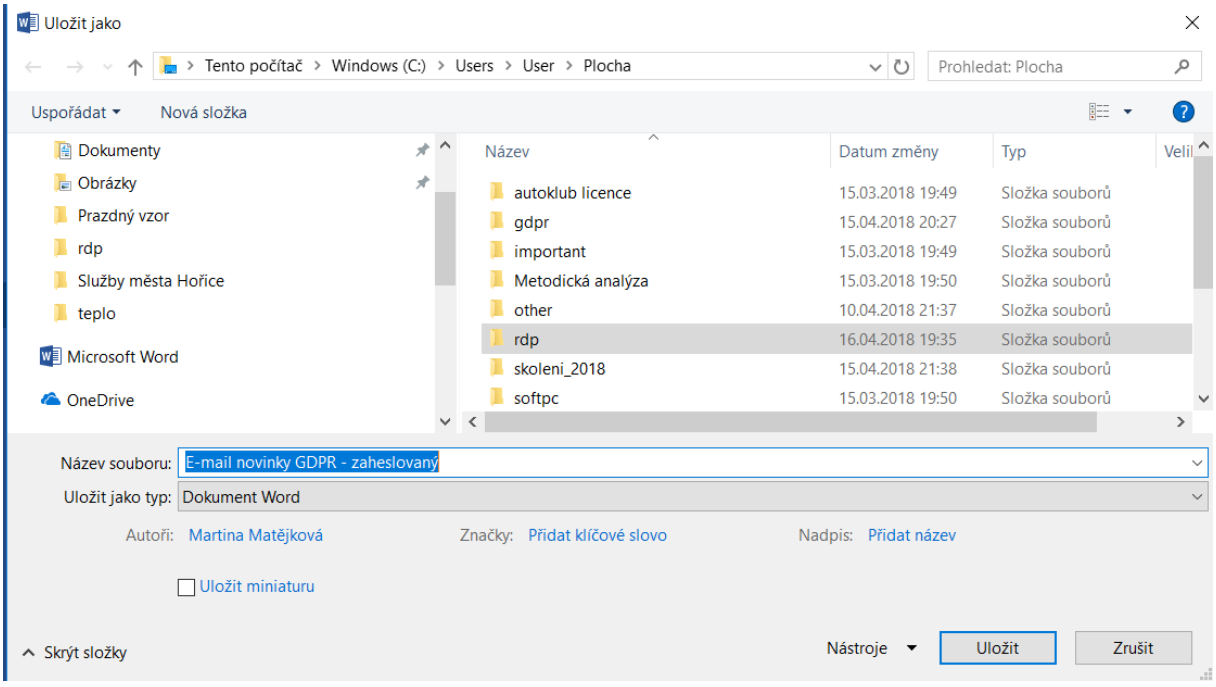
Vlastnoruční podpis klienta : …….....

V Hronově dne : ….....

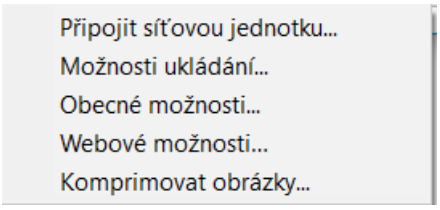
Varianta zabezpečení odesílaných příloh elektronickou poštou – doplnění souboru heslem

Jednou z variant, jak mohou pracovníci organizace zabezpečit elektronický soubor pro jeho zaslaní 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.

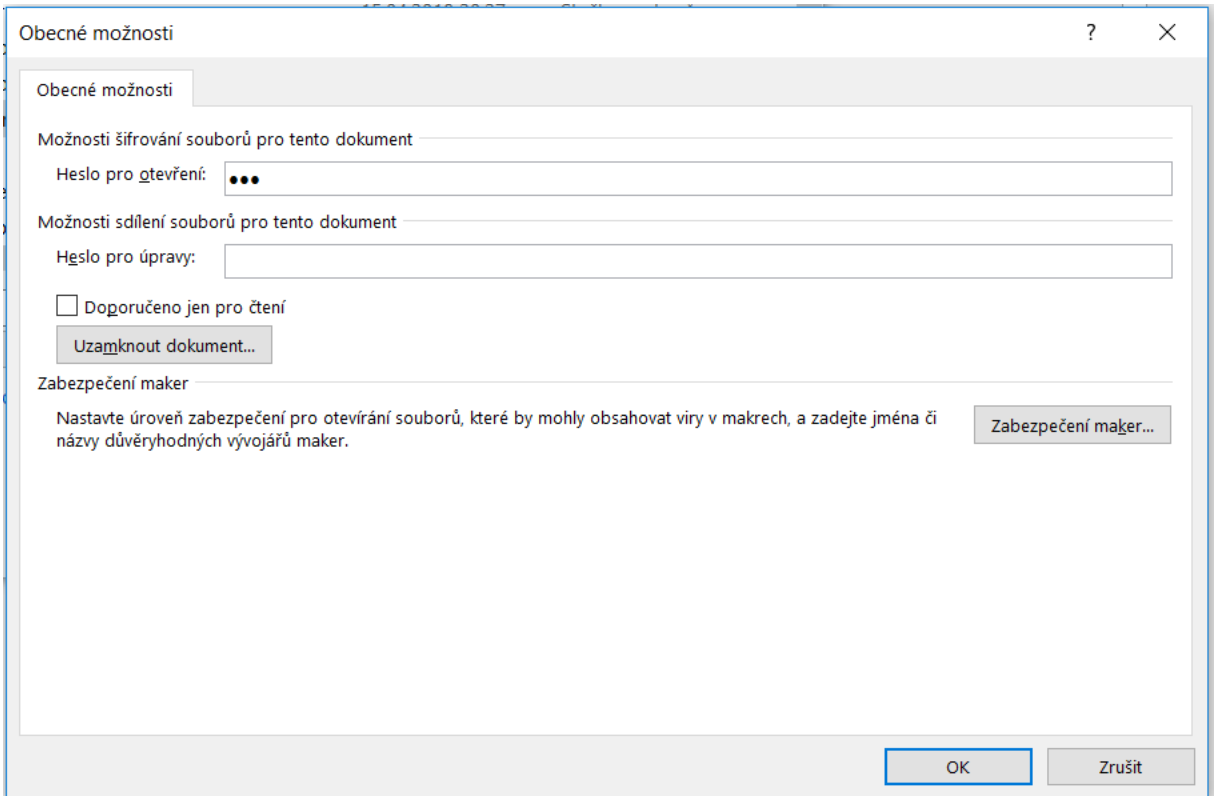
1. Vytvořený soubor uložíme přes funkci „Uložit jako“. Při ukládání zadáme název souboru s odlišným názvem než je původní, který si ponecháme ve svém počítači (tento zpravidla nebudeme doplňovat heslem pro jeho otevření).
2. Zvolíme nabídku „Nástroje“ a zde vybereme funkci „Obecné možnosti“.
3. V údaji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

Informační systém (jméno a výrobce)	**SQL Ekonom**
Popis software	pro vedení účetnictví, prodej zboží , evidenci majetku
Modul	došlé faktury, vydané faktury, pokladna, banka, majetek, účetnictví
Osobní údaje – základní	jméno, příjmení, adresa, Ič, Dič,telefon, email
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví, 235/2004 Sb. Zákon o DPH
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	Není
Možnosti exportů dat ze systému	Export do MS Word, MS Excel, Acrobat Reader
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Finanční úřad (kontrolní hlášení)
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, datový server umístěn v místnosti finanční účetní, přístup do software jištěn heslem v síle mimimálně 8 znaků(kombinace velkých a malých písmen a speciální znak), datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky

Zálohování dat a jejich zabezpečení	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Pracovní pozice s právem přístupu k osobním údajům	finanční účetní, ředitelka organizace
Anonymizace údajů po ukončení doby jejich zpracování	Ano
Má software certifikát souladu s GDPR	Ano

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	nejsou citlivé údaje, nízká úroveň rizika
Ztráta dat	2	nejsou citlivé údaje, nízká úroveň rizika
Zranitelnost	nejsou citlivé údaje, nízká úroveň rizika	systém zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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**
Popis software	pro výpočet výplat
Modul	mzdy a personalistika
Osobní údaje – základní	jméno, příjmení, bydliště, osobní číslo
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo, vznik a ukončení PP, číslo OP, rodinný stav, občanství, číslo bankovního účtu, zdravotní pojišťovna, údaje o penzijním či životním pojištění, děti – rodné číslo a datum narození, srážky ze mzdy, exekuce
Povinnost zpracovávat údaje na základě právního nároku	262/2006 Sb. Zákoník práce, 589/1992 Sb. Zákon o pojistném na soc.zab., 48/1997 Sb. Zákon o veř. zdravotním pojištění, 586/1992 Sb. Zákon o daních z příjmů
Povinnost zpracovávat údaje po dobu podle právního nároku	30 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 MS Word, MS Excel,Acrobat Reader
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	ČSSZ, Zdravotní pojišťovny,Finanční úřad
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, datový server umístěn v místnosti finanční účetní, přístup do software jištěn heslem v síle mimimálně 8 znaků(kombinace velkých a malých

	písmen a speciální znak), datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky
Zálohování dat a jejich zabezpečení	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Pracovní pozice s právem přístupu k osobním údajům	mzdová účetní, ředitelka organizace
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	hodně citlivých údajů, vyšší míra rizika
Ztráta dat	4	hodně citlivých údajů, vyšší míra rizika
Zranitelnost	2	systém zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 – MOBILNÍ TELEFONY

Informační systém (jméno a výrobce)	**Mobilní telefony**
Popis software	databáze kontaktů
Modul	
Osobní údaje – základní	jméno, příjmení, telefon, 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	po dobu platnosti kontaktu
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
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	PIN při spuštění nebo návratu z režimu spánku
Zálohování dat a jejich zabezpečení	data uložena pouze v mobilním telefonu
Pracovní pozice s právem přístupu k osobním údajům	ředitelka organizace
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	kontakty s nízkou citlivostí osobních dat
Ztráta dat	2	kontakty s nízkou citlivostí osobních dat
Zranitelnost	2	mobilní telefon jištěn PINem
Vnější hrozba	2	mobilní telefon jištěn PINem

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 – MS OUTLOOK, MOZILLA THUNDERBIRD

Informační systém (jméno a výrobce)	**MS Outlook, Mozilla Thunderbird**
Popis software	elektronická pošta
Modul	
Osobní údaje – základní	řada osobních údajů blíže nespecifikovaných
Osobní údaje – ostatní	řada osobních údajů blíže nespecifikovaných
Osobní údaje – citlivé	řada osobních údajů blíže nespecifikovaných
Povinnost zpracovávat údaje na základě právního nároku	oprávněný zájem
Povinnost zpracovávat údaje po dobu podle právního nároku	bez časového omezení
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	MS Word, MS Excel, Acrobat Reader
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, datový server umístěn v místnosti finanční účetní, datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky
Zálohování dat a jejich zabezpečení	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna

	kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Pracovní pozice s právem přístupu k osobním údajům	vedení organizace, finanční účetní, mzdová účetní, sociální pracovnice, zdravotní personál
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	4	hodně osobních dat s různým stupněm citlivosti
Ztráta dat	4	hodně osobních dat s různým stupněm citlivosti
Zranitelnost	2	počítač zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 – IS CYGNUS

Informační systém (jméno a výrobce)	**IS Cygnus**
Popis software	evidence sociální a zdravotní dokumentace klientů, stravovací provoz
Modul	
Osobní údaje – základní	jméno, příjmení, příjmení za svobodna, datum narození, rodné číslo, číslo občanky,evidence ZTP, bydliště, kontakty na blízké osoby (telefon, email), omezení ve svéprávnosti, kopie smlouvy, dodatky ke smlouvě, záznam o výši důchodu
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	zdravotní dokumentace
Povinnost zpracovávat údaje na základě právního nároku	Zákon č. 106/2006 Sb, o sociálních službách, na základě uzavření či plnění smlouvy
Povinnost zpracovávat údaje po dobu podle právního nároku	5 let nebo 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	MS Word,MS Excel
Předávání údajů jiným zpracovatelům	data částečně uložena na cloudovém uložišti zpracovatele, společnosti Iresoft s.r.o., za zálohu a zabezpečení produkčních dat odpovídá zpracovatel, revizní lékař
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, data

	částečně uložena na cloudovém uložišti zpracovatele, společnosti Iresoft s.r.o., datový server umístěn v místnosti finanční účetní, přístup do software jištěn heslem v síle mimimálně 8 znaků(kombinace velkých a malých písmen a speciální znak), datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky
Zálohování dat a jejich zabezpečení	
Pracovní pozice s právem přístupu k osobním údajům	vrchní zdravotní a sociální péče, sociální pracovník, ředitelka
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	osobní údaje citlivé s vyšším rizikem negativního dopadu na fyzickou osobu
Ztráta dat	3	osobní údaje citlivé s vyšším rizikem negativního dopadu na fyzickou osobu
Zranitelnost	2	počítač zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 – DOCHÁZKOVÝ A PŘÍSTUPOVÝ SW RON SOFTWARE

Informační systém (jméno a výrobce)	**Docházkový a přístupový software, RON software**
Popis software	evidence docházky zaměstnanců
Modul	
Osobní údaje – základní	jméno, příjmení, rodné číslo, titul, datum nástupu do zaměstnání
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	262/2006 Sb. Zákoník práce, 589/1992 Sb. Zákon o pojistném na soc. zabezpečení, 48/1997 Sb. Zákon o veř. zdravotním pojištění, 586/1992 Sb. Zákon o daních z příjmů
Povinnost zpracovávat údaje po dobu podle právního nároku	po dobu uzavřené pracovní 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	MS Word,MS Excel
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, datový server umístěn v místnosti finanční účetní, přístup do software jištěn heslem v síle mimimálně 8 znaků(kombinace velkých a malých písmen a speciální znak), datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky

Zálohování dat a jejich zabezpečení	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Pracovní pozice s právem přístupu k osobním údajům	ředitelka organizace
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	osobní údaje s nízkou citlivostí osobních dat
Ztráta dat	2	osobní údaje s nízkou citlivostí osobních dat
Zranitelnost	2	počítač zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 – PLÁN OŠETŘOVÁNÍ II, EZOPEREISIS

Informační systém (jméno a výrobce)	**Plán ošetřování II, EZOPEREISIS**
Popis software	tvorba plánu ošetřování
Modul	
Osobní údaje – základní	jméno, příjmení,
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	zdravotní dokumentace
Povinnost zpracovávat údaje na základě právního nároku	Zákon 372/2011 Sb. o Zdravotních službách, Vyhláška 98/2012 Sb. O zdravotnické dokumentaci
Povinnost zpracovávat údaje po dobu podle právního nároku	
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	MS Word,MS Excel
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	osobní údaje uloženy v databázi na datovém serveru společnosti, datový server umístěn v místnosti finanční účetní, přístup do software jištěn heslem v síle mimimálně 8 znaků(kombinace velkých a malých písmen a speciální znak), datový server jištěn proti vnějším hrozbám Firewallem na routeru na serveru,počítač chráněn antivirem ESET Internet security, heslo do počítače , heslo na spořič obrazovky
Zálohování dat a jejich zabezpečení	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna

	kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Pracovní pozice s právem přístupu k osobním údajům	zdravotní sestra
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	osobní údaje s nízkou citlivostí osobních dat
Ztráta dat	2	osobní údaje s nízkou citlivostí osobních dat
Zranitelnost	2	počítač zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	2	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 – KAMEROVÝ SYSTÉM BEZ ZÁZNAMU

Informační systém (jméno a výrobce)	**Kamerový systém bez záznamu**
Popis software	zajištění společných prostor pro neoprávněný vstup
Modul	
Osobní údaje – základní	obrazový záznam osob
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	
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
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití	bez uloženého záznamu
Zálohování dat a jejich zabezpečení	bez uloženého záznamu
Pracovní pozice s právem přístupu k osobním údajům	ředitelka organizace
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	1	osobní údaje s nízkou citlivostí osobních dat
Ztráta dat	1	osobní údaje s nízkou citlivostí osobních dat
Zranitelnost	1	počítač zabezpečen silným heslem, pravidelné provádění záloh, kontroly záloh
Vnější hrozba	1	datový server jištěn Firewallem, na serveru i stanicích antivirový program

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 - ÚČETNICTVÍ

Název dokumentu	**Účetnictví**
Popis dokumentu a účel dokumentu	došlé faktury, vydané faktury, pokladní doklady, bankovní výpisy pro vedení účetnictví
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, adresa, Ič,Dič, telefon, email
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	563/1991 Sb. Zákon o účetnictví 253/2004 Sb. Zákon o DPH
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	finanční účetní, ředitelka organizace
Předávání jiným zpracovatelům	ne
Předávání jiným příjemcům	Finanční úřad
Předávání osobních údajů do jiných zemí	ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič
Pracovní pozice s právem přístupu k osobním údajům	finanční účetní, ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna

	kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádu Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	nízké riziko, nejedná se o citlivé údaje
Ztráta dokumentu	2	nízké riziko, nejedná se o citlivé údaje
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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

Název dokumentu	**Mzdy**
Popis dokumentu a účel dokumentu	mzdové listy, důchodové listy, přihlášky a odhlášky k sociálnímu pojištění, výplatní pásky pro výplaty mezd pracovníkům
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, bydliště, jména děti, jméno manželky(a)
Osobní údaje – ostatní	pohlaví, rodinný stav
Osobní údaje – citlivé	rodné číslo, datum narození, vzdělání, zdravotní způsobilost, finanční situace, exekuce
Povinnost zpracovávat údaje na základě právního nároku	Zákoník práce 262/2006 Sb. 155/1995 Sb. Zákon o důchod.poj.
Povinnost zpracovávat údaje po dobu podle právního nároku	30 let
Evidence údajů nad právní rámec	ne
Bude vyžadován souhlas fyzické osoby (A/N)	ne
Pohyb dokumentu v rámci společnosti	mzdová účetní , ředitelka
Předávání jiným zpracovatelům	ne
Předávání jiným příjemcům	ČSSZ, Zdravotní pojišťovny
Předávání osobních údajů do jiných zemí	ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič

Pracovní pozice s právem přístupu k osobním údajům	mzdová účetní , ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	vysoce citlivá data s negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Ztráta dokumentu	4	vysoce citlivá data s negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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 - PERSONALISTIKA

Název dokumentu	**Personalistika (vedení lidí)**
Popis dokumentu a účel dokumentu	pracovní smlouva, platový výměr, žádost o zaměstnání, dotazník, vysvědčení, výpis z rejtříku trestů pro uzavření pracovně právního vztahu
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, bydliště, osobní číslo,
Osobní údaje – ostatní	pohlaví, rodinný stav
Osobní údaje – citlivé	rodné číslo, datum narození, vzdělání, zdravotní způsobilost
Povinnost zpracovávat údaje na základě právního nároku	Zákoník práce 262/2006 Sb. 155/1995 Sb. Zákon o důchodovém pojištění
Povinnost zpracovávat údaje po dobu podle právního nároku	30 let
Evidence údajů nad právní rámec	ne
Bude vyžadován souhlas fyzické osoby (A/N)	ne
Pohyb dokumentu v rámci společnosti	mzdová účetní, ředitelka
Předávání jiným zpracovatelům	ne
Předávání jiným příjemcům	ne
Předávání osobních údajů do jiných zemí	ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič

Pracovní pozice s právem přístupu k osobním údajům	mzdová účetní, ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	vysoce citlivá data s negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Ztráta dokumentu	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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 – SOCIÁLNÍ –VYJEDNÁVÁNÍ KONTRAKTU A ŘÍZENÍ SLUŽEB

Název dokumentu	**Sociální - vyjednání kontraktu a řízení služeb**
Popis dokumentu a účel dokumentu	prvokontakt, evidence žadatelů, lékařská zpráva, sociální šetření, individuální plánování, přijetí klienta, klient v sociální dokumentaci, klient ve zdravotní dokumentaci, klient v počítačové dokumentaci, úmrtí klienta, průkaz totožnosti, průkaz pojištěnce na zajištění služeb organizace pro klienty
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, bydliště
Osobní údaje – ostatní	jména rodinných příslušníků, telefon a email rodinných příslušníků
Osobní údaje – citlivé	rodné číslo, datum narození
Povinnost zpracovávat údaje na základě právního nároku	Zákon o sociálních službách 108/2006, Vyhláška 505/2006,Zákon ČNR o organizaci a provádění soc.zabezpečení 582/1991
Povinnost zpracovávat údaje po dobu podle právního nároku	Po dobu platnosti Smlouvy s klientem a po skončení 5 let
Evidence údajů nad právní rámec	fotografie klientů pro potřeby prezentace
Bude vyžadován souhlas fyzické osoby (A/N)	Ano
Pohyb dokumentu v rámci společnosti	sociální pracovníci, ředitelka společnosti
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Zdravotní pojišťovny, Městský úřad,
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn

	pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič
Pracovní pozice s právem přístupu k osobním údajům	socální pracovníci, ředitelka společnosti
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	3	středně vysoké riziko v citlivosti dat s možným negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Ztráta dokumentu	3	středně vysoké riziko v citlivosti dat s možným negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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

Název dokumentu	**Stravování**
Popis dokumentu a účel dokumentu	na zajištění stravovacího provozu pro klienty domova
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, osobní číslo
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Ne
Povinnost zpracovávat údaje na základě právního nároku	na základě uzavření a plnění smlouvy, 563/1991 Sb. Zákon o účetnictví
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	Ne
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	hospodářka, ředitelka
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič
Pracovní pozice s právem přístupu k osobním údajům	hospodářka, ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna

	kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	nízké riziko, nejedná se o citlivé údaje
Ztráta dokumentu	2	nízké riziko, nejedná se o citlivé údaje
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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 PRACOVNÍCH POMŮCEK

Název dokumentu	**Evidence pracovních pomůcek**
Popis dokumentu a účel dokumentu	karta pracovníka s nárokem na pracovní pomůcky pro evidenci vydaných pracovních pomůcek dle pracovníků
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	jméno, příjmení, osobní číslo pracovníka
Osobní údaje – ostatní	Nejsou
Osobní údaje – citlivé	Nejsou
Povinnost zpracovávat údaje na základě právního nároku	Zákoník práce 262/2006 Sb.
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	ředitelka, hospodářka
Předávání jiným zpracovatelům	Ne
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič

Pracovní pozice s právem přístupu k osobním údajům	hospodářka, ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	2	nízké riziko, nejedná se o citlivé údaje
Ztráta dokumentu	2	nízké riziko, nejedná se o citlivé údaje
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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 – ZDRAVOTNÍ DOKUMENTACE

Název dokumentu	**Zdravotní dokumentace**
Popis dokumentu a účel dokumentu	jméno, příjmení, diagnoza, výsledky vyšetření, rodné číslo, zdravotní pojišťovna pro zajištění zdravotních služeb klientům domova
Elektronická/Listinná/Obě verze	O
Osobní údaje – základní	Jméno, příjmení, datum narození, bydliště
Osobní údaje – ostatní	Ne
Osobní údaje – citlivé	Rodné číslo, další zdravotní údaje, zdravotní pojišťovna
Povinnost zpracovávat údaje na základě právního nároku	Zákon o zdravotních službách 372/2011, Vyhláška o zdravotnické dokumentaci 98/2012
Povinnost zpracovávat údaje po dobu podle právního nároku	10 let
Evidence údajů nad právní rámec	nahlížení do zdravotní dokumentace, poskytování informací o zdravotním stavu rodině, úschova zdravotní karty
Bude vyžadován souhlas fyzické osoby (A/N)	Ne
Pohyb dokumentu v rámci společnosti	zdravotní sestry, vrchni sestra
Předávání jiným zpracovatelům	lékař
Předávání jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru společnosti, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky

Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič
Pracovní pozice s právem přístupu k osobním údajům	vrchní sestra, zdravotní sestry, ředitelka
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádku Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	4	vysoce citlivá data s negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Ztráta dokumentu	4	vysoce citlivá data s negativním dopadem na fyzickou osobu v případe jejich zcizeni, zneužití
Zranitelnost	2	zálohování na externí disk, vyhrazený datový server s přístupem pouze oprávněných osob

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 oznamovatelů (Whistleblowing)

Název dokumentu	Evidence oznámení od oznamovatelů
Popis dokumentu a účel dokumentu	Agenda Whistleblowing
Elektronická/Listinná/Obě verze	Obě verze
Osobní údaje – základní	Jméno, příjmení, podpis, kontaktní adresa
Osobní údaje – ostatní	Ne
Osobní údaje - citlivé	Datum narození
Povinnost zpracovávat údaje na základě právního nároku	Směrnice Evropského Parlamentu a Rady (EU) 2019/1937
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
Pohyb dokumentu v rámci společnosti	Pověřená osoba
Předávání údajů jiným zpracovatelům	Ne
Předávání údajů jiným příjemcům	Ne
Předávání osobních údajů do jiných zemí	Ne
Způsob zabezpečení proti zneužití – elektronická verze	osobní údaje uloženy v osobních složkách na datovém serveru organizace, přístup na server zajištěn pouze odpovědným osobám, vnější přístup chráněn službou Firewall, heslo do PC minimálně 6 znaků písmena i čísla, heslo na spořič obrazovky
Způsob zabezpečení proti zneužití – listinná verze	uzamykatelná kancelář, uzamčena skříň, protipožární hlásič
Pracovní pozice s právem přístupu k osobním údajům	Pověřená osoba
Způsob archivace – elektronická verze	data jsou zálohována na externí disk NAS technologie každý den v nočních hodinách, 1x měsíčně je prováděna kontrola prováděných záloh správcem IT, zálohy jsou po 1 měsíci mazány, po době právního nároku jsou data v systému anonymizována
Způsob archivace – listinná verze	archivní dokumenty uzamčeny v samostatném archivu (spisovně), dokumenty po době právního nároku jsou

	předány do Státního archivu Náchod, skartace se provádí na Spisového a skartačního řádu Sd/16/2008

Stanovení rizik

Typ rizika	Úroveň rizika	Důvod rizika
Důležitost údajů	5	Dokumenty obsahují údaje s vysokou mírou citlivosti pro fyzickou osobu
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 a čím více citlivé osobní údaje obsahuje, tím vyšší známka.

Nápravná opatření pro snížení rizik

Poznámka