NAM SYSTEM
MONITORING TECHNOLOGY

Technologie pro dohledová a přijímací centra a GPS monitoring vozidel

INFORMACE O OCHRANĚ OSOBNÍCH ÚDAJŮ V SYSTÉMU

EmNET (RRH/IPC)

V.20200401

ÚČEL

Tento dokument popisuje dopad nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**Nařízení**“) a na něj navazujících právních předpisů na systém EmNET společnosti **NAM system, a.s.** se sídlem: U Pošty 1163/13, 735 64 Havířov – Prostřední Suchá, IČ: 25862731, číslo spisové značky: B 2365 – KS v Ostravě, a jeho používání.

Tento dokument popisuje role a práva a povinnosti jednotlivých osob, pokud jde o osobní údaje klientů a zaměstnanců uživatele nebo dalších osob, které mají vztah k uživateli, s výjimkou osobních údajů uživatele samotného. Uživatel je tedy ve vztahu k těmto osobním údajům povinen plnit veškeré povinnosti stanovené pro správce právními předpisy (tedy včetně Nařízení). **Uživatel však *není v postavení správce*, pokud jde o osobní údaje identifikující uživatele jako stranu smlouvy s provozovatelem, kontaktní údaje uživatele, údaje o poskytovaných službách, platební údaje a platební historie uživatele. Ve vztahu k těmto údajům je správcem provozovatel**, protože určil účely a prostředky zpracování osobních údajů. Zásady ochrany osobních údajů, jejichž správcem je provozovatel (viz část „Role: Uživatel systému EmNET“) naleznete na https://www.nam.cz/en/gdpr/

POPIS SYSTÉMU:

Technologie EmNET je speciálně vyvinutým bezpečnostním systémem pro ochranu a informování měkkých cílů o hrozbách. Ve své logické architektuře se EmNET skládá z jednotlivých klíčových prvků systému a jejich komunikačního propojení do jednoho celku. Řídící a koordinační částí systému EmNET je dispečerská aplikace RRH. Pro použití v terénu je určena mobilní aplikace EmNET-IPC.

TECHNICKÉ ŘEŠENÍ:

Technicky je systém tvořen HW a SW částí.

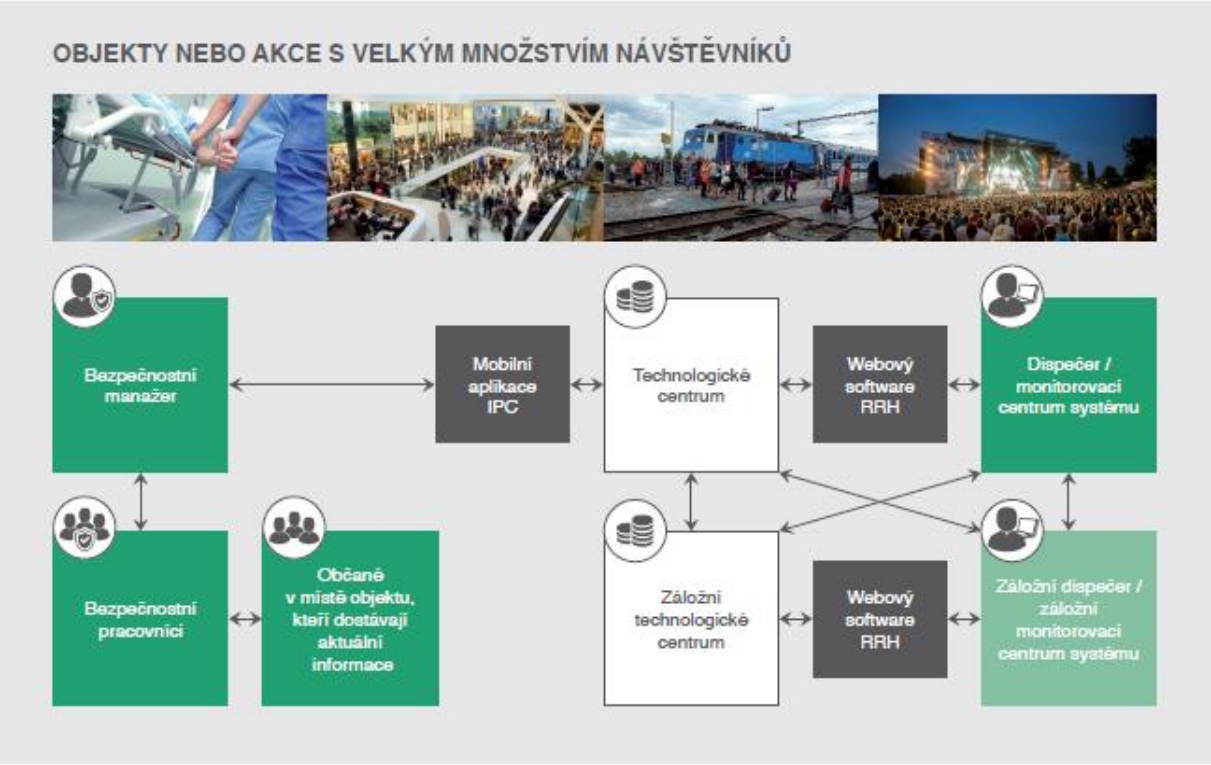
HW část zahrnuje různá provedení tísňových tlačítek (osobní/kapesní, náramek, pevná, tahová tlačítka/lišty apod.), různá provedení environmentálních detektorů (požární detektor, detektor zaplavení atd.) a různé typy GPS/SOS hodinek. Do HW části dále patří přijímače tísňových tlačítek a detektorů „REGGAE GTWbz“, které jsou pevně instalovány v objektech, v nichž je systém EmNET používán, a mobilní telefony personálu, který řeší vzniklé tísňové události (bezpečnostní manažeři, členové ostrahy objektu, vedení města, policie, apod.). V uvedených HW částech systému nejsou uloženy žádné osobní údaje.

SW část je tvořena:

- **serverová aplikace EmNET**
  - vyhodnocuje veškeré vniklé události v systému
  - dle nastavení zakládá akce
  - řídí odesílání notifikací
  - vyřizuje požadavky mobilních aplikací

  Pro správu serverové aplikace systému **EmNET** slouží webové rozhraní. Protože údaje o objektech a uživatelích systému jsou uloženy v databázi **serverové aplikace EmNET**, má legislativa v oblasti osobních údajů dopad právě na tuto SW část.

- **mobilní aplikace IPC**
  - instaluje se na mobilní telefony zasahujícího personálu
  - zpracovává notifikace a předává informace o vzniku událostí a hrozeb bezpečnostního charakteru uživatelům
  - po potvrzení akce zobrazuje údaje potřebné k vyřešení vniklé tísňové situace
  - lokálně neukládá žádné osobní údaje



JEDNOTLIVÉ ROLE V SYSTÉMU EmNET:

Pro posouzení systému EmNET z hlediska shody s pravidly pro ochranu osobních údajů je vhodné rozdělit systém do několika rolí a každou posuzovat samostatně:

ROLE: PROVOZOVATEL SYSTÉMU EmNET

Provozovatelem systému je společnost NAM system, a.s., která jej vyvinula a vyrábí i HW části tohoto systému. V systému vystupuje jako technologická společnost a z hlediska Nařízení je tzv. zpracovatelem osobních údajů. Zajišťuje bezproblémový chod HW, na kterém běží serverová aplikace EmNET, jeho bezpečnost, provádí administraci jednotlivých účtů uživatelů systému a zajišťuje technickou podporu a školení pro uživatele.

ROLE: UŽIVATEL SYSTÉMU EmNET

Uživatelem je organizace, která tento systém používá a je ve smluvním vztahu s provozovatelem systému. Zpravidla se jedná o organizace jako např. bezpečnostní agentury, městské policie, sociální úřady, obchodní centra a další. Provozovatel vytvoří uživateli samostatný izolovaný účet v systému s jedním přístupem s právem administrátora.

Z hlediska Nařízení je uživatel *správcem* osobních údajů předaných provozovateli uživatelem nebo třetí osobou jménem či z pověření uživatele nebo zadaných uživatelem či uvedenou třetí osobou do systému EmNET (jde o osobní údaje jeho klientů, zaměstnanců a dalších osob s výjimkou uživatele samotného). Uživatel je tedy ve vztahu k těmto osobním údajům povinen plnit veškeré povinnosti stanovené pro správce právními předpisy (tedy včetně Nařízení).

Uživatel však *není v postavení správce*, pokud jde o osobní údaje identifikující uživatele jako stranu smlouvy s provozovatelem, kontaktní údaje uživatele, údaje o poskytovaných službách, platební údaje a platební historie uživatele. Ve vztahu k těmto údajům je správcem provozovatel, protože určil účely a prostředky zpracování osobních údajů.

Uživatel/administrátor: Pomocí tohoto přístupu si uživatel může vytvořit další přístupy s právem administrátora nebo obsluhy, nadefinuje si své klienty s potřebnými údaji, přiřadí tísňová tlačítka, detektory, systém přijímačů a nastaví pravidla, jak se má celý systém pro tohoto uživatele chovat. Administrace účtu uživatele se provádí přes webové rozhraní systému a uživatel/administrátor je odpovědný i za zabezpečení počítače, z kterého administraci provádí.

Uživatel/obsluha: Jde o přístup do systému vytvořený uživatelem/administrátorem. Uživatel/obsluha má velmi omezená práva, určená pouze pro práci s webovou aplikací RRH v rozsahu potřebném pro poskytnutí pomoci v případě tísňové situace. Pomocí webové aplikace se může dostat k osobním údajům klienta, kterému poskytuje pomoc v tísňové situaci. Bezpečnost webové aplikace je zajištěna šifrovanou komunikací mezi aplikací a technologickým centrem.

ROLE: KLIENT (BEZPEČNOSTNÍ MANAŽER / MONITOROVÁNA OSOBA)

Osoba s přístupem k systému pomocí mobilní aplikace IPC nebo vybavená tísňovým tlačítkem nebo GPS/SOS hodinkami, které aktivuje pro přivolání pomoci v tísňové situaci. Anonymní rádiový signál např. z tísňového tlačítka je zachycen přijímačem v objektu a předán zabezpečenou trasou do technologického centra systému. Přijímače jsou vybaveny komunikátorem, který využívá vlastní datové APN bez prostupu do internetu.

Klient je subjektem údajů ve smyslu nařízení.

PRÁVNÍ ASPEKTY SYSTÉMU EmNET

Z hlediska Nařízení a dalších předpisů v oblasti ochrany osobních údajů a soukromí jsou jednotlivé role a odpovědnosti následující:

SPRÁVCE

Správcem ve smyslu Nařízení je uživatel systému EmNET. Uživatel je tedy povinen plnit veškeré povinnosti správce stanovené Nařízením a dalšími právními předpisy, pokud jde o osobní údaje obsažené v systému EmNET týkající se jeho klientů, zaměstnanců a dalších fyzických osob, jejichž osobní údaje uživatel do systému zavedl či jejich zavedení umožnil, s výjimkou osobních údajů, u kterých je správcem provozovatel (viz část „Role: Uživatel systému EmNET“). Uživatel je také povinen umožnit uvedeným subjektům výkon jejich práv. Jde mimo jiné o tyto povinnosti správce:

- dodržovat zásady zpracování osobních údajů,
- poskytnout subjektu údajů veškeré informace uvedené v článcích 13 a 14 Nařízení,
- umožnit každému subjektu údajů výkon jeho práv stanovených Nařízením,
- být schopen doložit soulad zpracování osobních údajů s Nařízením a dalšími právními předpisy.

ZPRACOVATEL

Zpracovatelem ve smyslu Nařízení je provozovatel systému EmNET, tedy společnost NAM system, a.s.

Vztah provozovatele a uživatele se řídí smlouvou, která zavazuje provozovatele (zpracovatele) vůči správci (tedy uživateli) a v níž je mj. stanoven předmět a doba trvání zpracování osobních údajů, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů a další práva a povinnosti stanovená v článku 28 Nařízení. Tato smlouva mimo jiné stanoví, že provozovatel zpracovává osobní údaje pouze na základě doložených pokynů uživatele (tedy správce ve smyslu Nařízení).

Provozovatel nepoužívá k provozu systému EmNET žádného dalšího zpracovatele osobních údajů. Pokud by v budoucnu zapojení dalšího zpracovatele do zpracování osobních údajů v systému EmNET bylo nutné, provozovatel tak učiní pouze s předchozí konkrétním nebo obecným písemným povolením správce (uživatele) a pouze na základě smlouvy mezi provozovatelem a dalším zpracovatelem, která uloží dalšímu zpracovateli stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě provozovatelem a uživatelem.

SUBJEKT ÚDAJŮ

Subjektem údajů ve smyslu Nařízení je:

- zaměstnanec uživatele, jehož osobní údaje jsou zpracovávány v systému EmNET,
- klient uživatele, jehož osobní údaje jsou zpracovávány v systému EmNET.

PRÁVNÍ DŮVOD A ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ:

Ve vztahu k zaměstnancům uživatele může být právním základem zpracování případ uvedený v článku 6 odst. 1, písm. f) Nařízení, tedy, že zpracování je nezbytné pro účely oprávněných zájmů příslušného správce. Těmito oprávněnými zájmy správce může být zájem na výkonu jeho podnikatelské činnosti, protože bez použití systému EmNET by správce (uživatel) nemohl poskytovat služby svým klientům s takovém rozsahu a kvalitě, jako s použitím tohoto systému.

Ve vztahu ke klientům uživatele může být právním základem zpracování případ uvedený v článku 6 odst. 1, písm. b) Nařízení, tedy, že zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, a není-li tento právní základ ve vztahu k některým či všem osobním údajům klienta dán, pak článku 6 odst. 1, písm. a) Nařízení, tedy, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů. Avšak pokud, jsou v systému EmNET zpracovávány správcem osobní údaje, které spadají do zvláštních kategorií osobních údajů (údaje o zdravotním stavu klientů), může být právním základem zpracování výhradně případ uvedený v článku 6 odst. 1, písm. a) Nařízení, tedy, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.

Správce je povinen zajistit:

- Právní základ pro zpracování osobních údajů dle Nařízení;
- aby veškeré osobní údaje byly shromažďovány a předávány provozovateli zákonným způsobem;
- nevydat žádné pokyny provozovateli, které by byly jakýmkoliv způsobem v rozporu s Nařízením nebo zákonnými právy subjektů údajů;
- jednat jako kontaktní místo subjektu údajů.

PŘÍNOSY ZPRACOVÁNÍ

Používaní systému HelpCare přináší benefity jak uživateli, tak jeho klientům i zaměstnancům.

Přínos pro	**Popis přínosu**
uživatele	možnost efektivně poskytovat služby klientům
uživatele	možnost získat nové klienty
uživatele	prokázání řádného a soustavného poskytování služeb klientům
uživatele	snížení možnosti nesprávného nebo nekvalitního poskytování služeb klientům
zaměstnance uživatele	pomoc při plnění povinností z pracovněprávního vztahu
klienty	kvalitnější služby ze strany uživatele
klienty	prokázání vadného poskytnutí služby ze strany uživatele

RIZIKA ZPRACOVÁNÍ

Jako každé zpracování osobních údajů nese i používání systému EmNET určitá rizika pro práva a svobody subjektů údajů, tedy zejména klientů či zaměstnanců uživatele. Jedním ze stěžejních principů Nařízení je přístup založený na riziku, který znamená, že správce (tedy uživatel) musí posouzení připravovaného zpracování osobních údajů vzít v úvahu všechna rizika pro práva a svobody fyzických

osob. To samozřejmě zahrnuje i rizika v kontextu bezpečnostních opatření. To lze ilustrovat na zásadě přesnosti; čím vyšší je (jakékoli) riziko plynoucí z nepřesnosti některého ze zpracovávaných osobních údajů, tím větší jsou nároky na mechanismy aktualizace osobních údajů.

„Rizikem“ se rozumí scénář, v němž je uveden popis určité události (hrozby) a jejích důsledků (újma) společně s odhadem její závažnosti a pravděpodobnosti. Nařízení ukládá správci povinnost zavést odpovídající opatření, aby zajistil a byl schopen doložit soulad s Nařízením, přičemž přihlíží mimo jiné k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob.

Hrozbami pro práva a svobody subjektů údajů v souvislosti s používáním systému EmNET mohou například být:

Hrozba	**Příklad hrozby (pro systém EmNET)**	**Protiopatření provozovatele**
Zpracování nepřesných osobních údajů	V systému jsou neaktualizované osobní údaje	Ve smlouvách o poskytování služby EmNET musí být obsaženo ujednání, že uživatel je povinen hlásit neprodleně provozovateli každou změnu svých osobních údajů.
Zpracování osobních údajů nad rámec účelu	Osobní údaje shromážděné pro účel poskytování služby jsou následně použity pro přímý marketing nesouvisejícího zboží nebo předávány novému příjemci.	Provozovatel zpracovává osobní údaje klientů a zaměstnanců uživatele pouze za účelem poskytování služby HelpCare. Provozovatel zpracovává osobní údaje klientů a zaměstnanců uživatele pouze na základě smlouvy s uživatelem, která splňuje požadavky Nařízení na smlouvu o zpracování osobních údajů.
Zpracování osobních údajů bez právního základu	V systému jsou osobní údaje osob, které neuzavřely smlouvu s provozovatelem	Vnitřní předpis provozovatele stanoví, že služby mohou být poskytovány výhradně osobám, které uzavřely s provozovatelem smlouvu.

Zpracování osobních údajů neočekávané subjektem údajů	Data klientů jsou využívána pro marketingové účely.	Smlouva o zpracování stanoví pro provozovatele striktní omezení nakládání s osobními údaji.
Ztráta osobních údajů	Dojde k poškození úložiště dat, které způsobí nemožnost přístupu k nim.	Zákaz přenosu dat ze serverů na lokální úložiště. Zálohování.
Krádež osobních údajů	Hackerský útok.	Strategie hloubkové obrany.
Zneužití přístupu k osobním údajům	Administrátor neoprávněně zkopíruje kontaktní údaje klientů a předá je třetí osobě za účelem nabídky zboží nebo služeb.	Nastavení oprávnění přístupu k osobním údajům. Smlouvy o mlčenlivosti. Logování činností.

Společnost NAM system, a.s., jakožto zpracovatel osobních údajů v systému EmNET provedla posouzení a zhodnocení rizik zpracování osobních údajů v systému EmNET, jak při činnostech provozovatele, tak i uživatele, které je přílohou č. 1 těchto zásad.

Společnost NAM system, a.s., jakožto zpracovatel osobních údajů v systému EmNET přijala v těchto pravidlech uvedená opatření, které minimalizuji riziko ztráty či krádeže osobních údajů nebo zneužití přístupu k nim v těch částech systému EmNET, jenž jsou pod její kontrolou.

Správce (tedy uživatel) je povinen přijmout účinná opatření proti riziku ztráty či krádeže osobních údajů nebo zneužití přístupu k nim v těch částech systému EmNET, které jsou pod jeho kontrolou, zejména zajistit bezpečnost a omezení přístupu k je výpočetní technice a mobilním zařízením zapojeným do systému EmNET, aby bylo zabráněno náhodnému nebo protiprávnímu zničení, ztrátě, pozměňování, neoprávněnému zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněnému přístupu k nim.

Správce je též povinen přijmout účinná opatření proti všem ostatním rizikům pro práva a svobody fyzických osob v souvislosti se zpracováním osobních údajů v systému EmNET.

Je nezbytné upozornit, že pokud uživatel hodlá používat systém EmNET k systematickému monitorování zaměstnanců nebo zpracování zdravotnických údajů klientů[1], je uživatel povinen před započetím těchto činností provést tzv. posouzení vlivu na ochranu osobních údajů a zpracování provádět až dle výsledků tohoto posouzení.

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ PROVOZOVATELE K ZABEZPEČENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOULADU S POŽADAVKY NAŘÍZENÍ A ZAJIŠTĚNÍ OCHRANY PRÁV SUBJEKTU ÚDAJŮ

Vzhledem ke stavu techniky, nákladům na realizaci a podstatě, rozsahu, kontextu a účelům zpracování osobních údajů, jakož i k různé pravděpodobnosti a závažnosti rizik pro práva a svobody fyzických osob

[1] protože tato činnost je považována za vysoce rizikovou pro práva a svobody subjektů údajů

provozovatel přijal níže uvedená technická a organizační opatření k zabezpečení zpracování osobních údajů v souladu s požadavky Nařízení a k zajištění ochrany práv subjektů údajů:

1. Serverová část je umístěna v zabezpečeném technologickém centru v souladu s platnou legislativou. Fyzický přístup do technologického centra mají pouze pověření zaměstnanci společnosti NAM system, a.s., kteří uzavřeli smlouvou o mlčenlivosti a ochraně informací. Společnost NAM system, a.s. je držitelem certifikátu Národního bezpečnostního úřadu.
2. Technicky je chod centra zajištěn několikanásobným jištěním napájecích zdrojů a pokročilým systémem hloubkové obrany. Strategie hloubkové obrany zajišťuje, že bezpečnostní kontroly jsou přítomny v různých vrstvách služby a že pokud některá oblast selže, existují kompenzační kontroly, které udržují bezpečnost po celou dobu. Strategie také zahrnuje taktiky, jak odhalit, předcházet a zmírnit narušení bezpečnosti dříve, než k nim dojde. To zahrnuje též neustálé zlepšování funkcí zabezpečení služby, včetně:
    - Šifrování dat
    - Zálohování dat
    - Monitorování síťového provozu
    - Pravidelné aktualizace zabezpečení
    - Detekce a prevence rizik na úrovni sítě
    - Multifaktorová autentizace pro přístup k službám
    - Audit přístupů a činností administrátora
    - Kontinuální zvyšování úrovně odborných znalostí administrátorů
3. Zabránění porušení těchto pravidel zahrnuje také řízené mazání nepotřebných účtů, když zaměstnanec provozovatele odchází, mění skupiny nebo nepoužije účet před jeho vypršením. Kdykoli je to možné, zásah člověka je nahrazen automatizovaným procesem založeným na nástrojích, včetně rutinních funkcí, jako je nasazení, ladění, diagnostika a restartování.
4. Kontrola fyzického přístupu do technologického centra využívá více autentifikačních a bezpečnostních procesů, včetně čipových karet, místních bezpečnostních pracovníků, nepřetržitého sledování videa a dvoufaktorové autentizace. Technologické centrum je monitorováno pomocí pohybových senzorů. Pro případ přírodních katastrof zahrnuje zabezpečení také automatizované protipožární a hasicí systémy.
5. Data uživatelů a klientů nejsou provozovatelem předávána žádné třetí straně (marketing, obchodní nabídky apod.) s výjimkou případů, kdy by to bylo provozovateli uloženo rozhodnutím orgánu veřejné moci a provozovatel systému data nezpracovává žádnými jinými způsoby, než které jsou nezbytné pro fungování služby.
6. Společnost NAM system, a.s. jakožto zpracovatel osobních údajů přijala opatření ve formě vnitřního předpisu pro zajištění toho, aby její zaměstnanci (jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele), kteří mají přístup k osobním údajům, zpracovávaly osobní údaje v souladu pravidly uvedenými v těchto zásadách a s Nařízením.
7. S výjimkou odstavce 8. níže přestane provozovatel po ukončení smlouvy s uživatelem zpracovávat osobní údaje zpracovávané jménem uživatele. Na základě písemného pokynu uživatele dále provozovatel zajistí na náklady uživatele vrácení uživateli veškerých osobních údajů společně se všemi kopiemi, které vlastní, nebo drží. Nepředloží-li uživatel pokyn k vrácení do dvou (2) měsíců ode dne ukončení smlouvy, provozovatel smí vymazat veškeré osobní údaje, včetně jejich kopií, pokud není uchovávání osobních údajů požadováno právními předpisy. Mají-li být osobní údaje vráceny v souladu s výše uvedeným, budou vráceny v běžném čitelném formátu, na kterém se strany dohodnou.
8. Provozovatel si smí ponechat osobní údaje v rozsahu požadovaném právními předpisy EU nebo členského státu pouze v rozsahu a po dobu odpovídající ustanovením právních předpisů EU nebo členského státu, a vždy za předpokladu, že provozovatel zajistí důvěrnost veškerých osobních údajů a zajistí, aby byly tyto osobní údaje zpracovávány pouze v nutném rozsahu

podle účelu specifikovaného právními předpisy EU nebo členského státu požadujícími jejich uchovávání, a ne pro jakýkoli jiný účel.

9. Zpracovatel jmenoval pověřence pro ochranu osobních údajů podle článku 37 Nařízení. Kontaktní údaje pověřence jsou uvedeny na https://www.namsystem.com/gdpr/
10. Zpracovatel vede záznamy o všech kategoriích činností zpracování prováděných pro správce v souladu s ustanovením článku 30 odst. 2. Nařízení.

Blíže jsou technická a organizační opatření k zabezpečení zpracování osobních údajů přijatá provozovatelem popsána v příloze č. 2 těchto zásad.

PŘÍLOHY:

1) Riziková matice – EmNET
2) Technická a organizační opatření k zabezpečení zpracování osobních údajů

Riziková matice – EmNET

Újma	Hrozba	Protiprávní shromažďování nebo nakládání s osobními údaji Nepřesnost údajů Zpracování nad rámec účelu Zpracování bez právního základu Zpracování neočekávané subjektem údajů			Porušení zabezpečení Ztráta dat Krádež dat Zneužití přístupu			Celkem
		Pravděpodobnost	Závažnost	Skóre	Pravděpodobnost	Závažnost	Skóre	Míra rizika
Hmotná újma								
Ublížení na zdraví		0		0	0		0	0
Krádeži či zneužití identity		0		0	0		0	0
Finanční ztráta		0		0	0		0	0
Významné hospodářské znevýhodnění		0		0	0		0	0
Jiná hmotná škoda		0		0	0		0	0
Nehmotná újma								0
Porušení ochrany podoby člověka		0		0	0		0	0
Porušení soukromí		0		0	3	5	15	15
Ztráta kontroly na osobními údaji		3	3	9	1	4	4	13
Porušení listovního tajemství		0		0	0		0	0
Obtěžování (nevyžádané zprávy)		0		0	0		0	0
Poškození pověsti		0		0	0		0	0
Psychická újma		2	1	2	0		0	2
Diskriminace		0		0	0		0	0
Nadměrné sledování		3	3	9	0		0	9
Ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím		0		0	0		0	0
Neoprávněné zrušení pseudonymizace		0		0	0		0	0
Významné společenské znevýhodnění		0		0	0		0	0
Jiná nehmotná újma		0		0	0		0	0

Legenda:
Rozsah "Pravděpodobnosti" od 0 (nemožné) po 10 (jisté)
Rozsah "Závažnosti" od 0 (žádná) po 10 (velmi vysoká)

Celková míra rizika tohoto zpracování	**39**

Příloha č. 2 Zásady ochrany osobních údajů EmNET

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ K ZABEZPEČENÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. ŘÍZENÍ PŘÍSTUPU DO MÍST ZPRACOVÁNÍ

Provozovatel zavedl níže uvedená technická a organizační opatření, která znemožní neoprávněným osobám vstup do míst a k zařízením, kde dochází ke zpracování osobních údajů.

Technická a organizační opatření pro řízení přístupu osob do míst zpracování osobních údajů mohou být následující:

- Ochranná opatření pro zamezení krádeže, manipulace a škod na zařízení používaném pro zpracování údajů;
- Bezpečnostní zónování objektu;
- Přihlášení (logování) personálu na daném pracovišti;
- Řízený výdej klíčů (včetně přístupových oblastí);
- Fyzická ostraha v režimu 24/7/365;
- Bezpečnostní dokumentace;
- Monitorovací zařízení, např. poplachový systém, sledování pomocí kamerového systému.

2. ŘÍZENÍ PŘÍSTUPU K SERVEROVÉ APLIKACI HEPLCARE

Provozovatel zavedl níže uvedená technická a organizační opatření, která znemožní neoprávněným osobám přístup k osobním údajům, které jsou zpracovávány v serverové aplikaci EmNET. Neoprávněné osoby nemají přístup k serverové aplikaci EmNET.

Technická a organizační opatření zajišťující identifikaci uživatele v systému mohou být následující:

- Fyzický přístup do technologického centra mají pouze pověření zaměstnanci provozovatele, kteří uzavřeli smlouvou o mlčenlivosti a ochraně informací
- Přístupová oprávnění (hesla, kódy apod.);
- Bezpečnostní monitoring (logování administrátorů a uživatelů);
- Automatické zamykání (např. heslo požadované pro opětovné přihlášení);
- Nastaven proces zajišťující okamžité odvolání veškerých přístupových práv v případě, že zaměstnanec ukončí pracovní proces;
- Bezpečnostní zálohy;
- Antivirová ochrana;
- Šifrování;
- Firewall;
- Kontinuální zvyšování úrovně odborných znalostí administrátorů;
- Bezpečnostní dokumentace.

3. ŘÍZENÍ PŘÍSTUPU K ÚDAJŮM

Provozovatel zajistil, aby osoby oprávněné používat systém EmNET měly přístup pouze k údajům, ke kterým mají přístupové právo. Dále provozovatel zajistil, aby tyto údaje nemohly být v serverové aplikaci EmNET neoprávněnou osobou přečteny, kopírovány, změněny či vymazány během jejich zpracování, používání a dalšího přechovávání.

Opatření k přístupovým a přihlašovacím právům a jejich monitorování jsou následující:

- Nastavení přístupových oprávnění, dle konkrétních potřeb (odlišné úrovně přístupů k údajům);
- Úložiště údajů jsou umístěna v zabezpečených místnostech, které jsou pravidelně kontrolovány z hlediska bezpečnosti;
- Dodržují se zásady need to know (zpřístupnit minimum potřebných informací);
- Neznámý / neoprávněný software nelze instalovat na hardware poskytovatele;
- Údaje jsou přechovávány šifrované;
- Bezpečnostní dokumentace.

4. ŘÍZENÍ PŘENOSU

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěno, že během digitálního přenosu nebo dopravy / přechovávání na nosičích dat pro přenos nesmějí být údaje přečteny, kopírovány, změněny ani vymazány.

Opatření během přenosu, dopravy a přechovávání údajů na nosičích dat jsou následující:

- Přístupová opatření (hesla, kódy apod.);
- Šifrování;
- Kódování, síťové připojení (VPN = Virtual Network/virtuální soukromá síť);
- Digitální podpis;
- Bezpečnostní monitoring uživatelů;
- Opatření pro zamezení neřízeného přenosu údajů (např. zamykání portů USB);
- Bezpečnostní dokumentace.

5. ŘÍZENÍ ZÁZNAMŮ

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěna kontrola, zda byly údaje v systému zpracování údajů zadány, změněny nebo vymazány, a kým.

Opatření pro následné ověření, zda byly údaje zadány, změněny nebo vymazány, a kým jsou následující:

- Bezpečnostní monitoring uživatelů (čtení, změna, pokusy o neoprávněný přístup apod., pravidelná analýza záznamů / speciální analýza záznamů, bude-li třeba);
- Pravidelné vyhodnocování bezpečnostního monitoringu;
- Bezpečnostní dokumentace.

6. ŘÍZENÍ ZPRACOVÁNÍ ÚDAJŮ

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěno, že osobní údaje budou zpracovávány pouze v souladu se smlouvou uzavřenou s uživatelem.

Opatření pro odlišení povinností ve vztahu k uživateli jsou následující:

- Zaměstnanci provozovatele jsou povinni odlišovat zpracování údajů provozovatele, uživatele a dalších zákazníků provozovatele (dalších uživatelů);
- S údaji uživatele je provozovatelem nakládáno minimálně se stejnou péčí jako s vlastními "důvěrnými" údaji provozovatele;
- opatření ve formě vnitřního předpisu provozovatele pro zajištění toho, aby jeho zaměstnanci (jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele), kteří mají přístup k osobním údajům, zpracovávaly osobní údaje v souladu pravidly uvedenými v těchto zásadách a s Nařízením;

- Provozovatel jmenoval pověřence na ochranu osobních údajů;
- Záznamy o činnostech zpracování provozovatele.

7. ŘÍZENÍ DOSTUPNOSTI ÚDAJŮ

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěno, že osobní údaje systému EmNET budou chráněny proti náhodnému zničení nebo ztrátě.

Opatření pro zajištění zamezení zničení / ztráty údajů jsou následující:

- Zálohování;
- Oddělené přechovávání;
- Provádění zrcadlového otisku disků (např. postup RAID);
- Několikanásobné jištění napájecích zdrojů;
- Pravidelná kontrola stavu systému (monitorování);
- Antivirová ochrana;
- Nouzový plán (včetně pravidelných zkoušek);
- Automatizované protipožární a hasicí systémy
- Monitorování síťového provozu
- Pravidelné aktualizace zabezpečení
- Detekce a prevence rizik na úrovni sítě

8. ŘÍZENÍ ODDĚLENÍ ZPRACOVÁNÍ

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěno, že zpracovávání a přechovávání osobních údajů nashromážděných pro určitý účel odděleně od jakýchkoliv jiných dat.

Opatření pro zajištění odděleného zpracování osobních údajů (přechovávání, změna, výmaz, přenos), pokud byly osobní údaje nashromážděny z odlišných důvodů, přijatá provozovatelem jsou následující:

- Víceklientské řešení;
- Oddělení systémů v reálném čase a vyzkoušení prostředí;
- Dokumentované oddělení funkcí.
- Data uživatelů a klientů nejsou provozovatelem předávána žádné třetí straně (marketing, obchodní nabídky apod.) s výjimkou případů, kdy by to bylo provozovateli uloženo rozhodnutím orgánu veřejné moci a provozovatel systému data nezpracovává žádnými jinými způsoby, než které jsou nezbytné pro fungování služby