NAM SYSTEM
MONITORING TECHNOLOGY

Technologie pro dohledová a přijímací centra a GPS monitoring vozidel

PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ

ONI system

V.20180510

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 ONI system 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 uživatelů vozidel (nebo jiných objektů) zákazníka (zejména zaměstnanci zákazníka nebo klienti zákazníka), s výjimkou osobních údajů zákazníka samotného. Zákazník je tedy ve vztahu k těmto osobním údajům povinen plnit veškeré povinnosti stanovené pro správce (jak jej definuje Nařízení) právními předpisy (tedy včetně Nařízení). **Zákazník však *není v postavení správce*, pokud jde o osobní údaje identifikující zákazníka jako stranu smlouvy s provozovatelem, kontaktní údaje zákazníka, údaje o poskytovaných službách, platební údaje, dodací údaje (včetně údajů o montáži a servisu), fakturační údaje a platební historie zákazníka. 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: zákazník ONI systemu“) naleznete zde.

POPIS SYSTÉMU:

ONI system je systém pro sledování, střežení a navigaci mobilních objektů, zejména vozidel, věcí a osob. Hlavní funkcí systému je zaznamenávání poloh, provozních stavů a událostí jednotlivých objektů registrovaných v ONI systemu. Zákazníkovi rovněž poskytuje přehled, k jakým situacím došlo, kdy a kde se staly, a umožňuje jejich vyhodnocení (sledování spotřeby pohonných hmot, tvorbu knihy jízd, evidenci docházky atp.).

NAM SYSTEM
MONITORING TECHNOLOGY

Technologie pro dohledová a přijímací centra a GPS monitoring vozidel

TECHNICKÉ ŘEŠENÍ:

Technicky je systém tvořen HW a SW částí.

HW část zahrnuje různá provedení GPS jednotek umísťovaných do objektů či na ně a různá provedení detektorů (detektor hladiny pohonných hmot atd.). V uvedených HW částech systému nejsou uloženy žádné osobní údaje.

SW část je tvořena:

serverovou aplikací ONI system. Pro její správu slouží webové rozhraní a mobilní aplikace:

- **webové rozhraní** ONI system (není u zařízení TICK)
  - vyhodnocuje veškeré vzniklé události zaznamenané GPS nebo rádiovými jednotkami
  - dle nastavení zasílá informační notifikace
  - zobrazuje změny provedené v mobilní aplikaci

- **mobilní aplikace** ONI system
  - instaluje se na mobilní telefony zákazníků
  - lokálně neukládá žádné osobní údaje

NAM system, a.s.
U Pošty 1163/13
735 64 Havířov – Prostřední Suchá
Česká republika

Telefon: +420 596 531 140
Internet: www.nam.cz
E – mail: info@nam.cz

Banka: ČSOB Orlová č.ú. 167656634/0300
Zapsán v OR u KS Ostrava Rg. B 2365
IČO: 25862731
DIČ: CZ25862731

JEDNOTLIVÉ ROLE V ONI SYSTEMU

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

ROLE: PROVOZOVATEL ONI SYST EMU

Provozovatelem ONI systemu je společnost NAM system, a.s., která jej vyvinula a vyrábí i HW části tohoto systému. Zajišťuje bezproblémový chod HW, na kterém běží serverová aplikace, jeho bezpečnost, provádí administraci jednotlivých účtů zákazníků systému a zajišťuje technickou podporu a školení pro zákazníky.

ROLE: ZÁKAZNÍK ONI SYST EMU

Zákazníkem je organizace, která tento systém používá a je ve smluvním vztahu s provozovatelem systému. Provozovatel vytvoří uživateli samostatný izolovaný účet v systému s jedním přístupem s právem administrátora.

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

Zákazník však *není v postavení správce*, pokud jde o osobní údaje identifikující zákazníka jako stranu smlouvy s provozovatelem, údaje o poskytovaných službách, platební údaje, dodací údaje (včetně údajů o montáži a servisu), fakturační údaje a platební historie zákazníka. Ve vztahu k těmto údajům je správcem provozovatel, protože určil účely a prostředky zpracování osobních údajů.

Administrace účtu zákazníka se provádí přes webové rozhraní systému (tento účet není zákazníkovi ani uživateli dostupný u služeb poskytovaných prostřednictvím zařízení TICK) a zákazník je odpovědný i za zabezpečení počítače, z kterého administraci provádí. Zákazník se pomocí webového rozhraní či mobilní aplikace se může dostat k osobním údajům uživatelů. Bezpečnost webového rozhraní a mobilní aplikace je zajištěna na úrovni podporovaných verzí operačního systému počítače a mobilního telefonu a šifrovanou komunikací mezi aplikací a technologickým centrem.

ROLE: UŽIVATEL

Osoba užívající vozidlo či jiný objekt nebo osoba vybavená jednotkou ONI system. Anonymní signál jednotky je doručen zabezpečenou trasou do technologického centra systému. Jednotky ONI system jsou vybaveny komunikátorem, který využívá vlastní datové APN bez prostupu do internetu.

Uživatel je subjektem údajů ve smyslu nařízení.

PRÁVNÍ ASPEKTY ONI SYSTEMU

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 zákazník ONI system. Zákazník je tedy povinen plnit veškeré povinnosti správce stanovené Nařízením a dalšími právními předpisy, pokud jde o osobní údaje obsažené v ONI system týkající uživatelů vozidel (nebo jiných objektů) zákazníka (zejména zaměstnanci zákazníka nebo klienti zákazníka) a dalších fyzických osob, jejichž osobní údaje zákazník do systému zavedl či jejich zavedení umožnil, s výjimkou osobních údajů, u kterých je správcem provozovatel (viz část „Role: zákazník ONI systemu“). Zákazník je také povinen umožnit uvedeným subjektům (uživatelům) 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 ONI systemu, tedy společnost NAM system, a.s.

Vztah provozovatele a zákazníka se řídí smlouvou, která zavazuje provozovatele (zpracovatele) vůči správci (tedy zákazníkovi) 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 zákazníka (tedy správce ve smyslu Nařízení).

Provozovatel nepoužívá k provozu ONI systemu žádného dalšího zpracovatele osobních údajů. Pokud by v budoucnu zapojení dalšího zpracovatele do zpracování osobních údajů v ONI systemu bylo nutné, provozovatel tak učiní pouze s předchozí konkrétním nebo obecným písemným povolením správce (zákazníka) 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 zákazníkem.

SUBJEKT ÚDAJŮ

Subjektem údajů ve smyslu Nařízení je uživatel objektu registrovaného v ONI systemu, tedy:

- zaměstnanec zákazníka, jehož osobní údaje jsou zpracovávány v ONI systemu,
- klient zákazníka, jehož osobní údaje jsou zpracovávány v ONI systemu.

PRÁVNÍ DŮVOD A ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ:

Ve vztahu k zaměstnancům zákazníka 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 ochrana majetku zákazníka, bezpečnost provozu vozidla - ochrana zdraví v případě dopravní nehody a vedení knihy jízd pro daňové účely a též zájem na výkonu jeho podnikatelské činnosti, protože bez použití ONI systemu by správce (zákazník) nemohl poskytovat služby svým klientům v takovém rozsahu a kvalitě, jako s použitím tohoto systému.

Ve vztahu ke klientům zákazníka 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.

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 ONI systemu přináší benefity jak zákazníkům, tak jeho klientům i zaměstnancům.

Přínos pro	**Popis přínosu**
celou společnost	úspory pohonných hmot
zákazníka	možnost efektivně poskytovat služby klientům
zákazníka	možnost získat nové klienty
zákazníka	prokázání řádného a soustavného poskytování služeb klientům
zákazníka	snížení možnosti nesprávného nebo nekvalitního poskytování služeb klientům
zákazníka	ochrana majetku zákazníka
zákazníka	vedení knihy jízd pro daňové účely
zaměstnance zákazníka	pomoc při plnění povinností z pracovněprávního vztahu
zaměstnance zákazníka	ochrana zdraví v případě dopravní nehody
klienty	kvalitnější služby ze strany zákazníka
klienty	prokázání vadného poskytnutí služby ze strany zákazníkem
klienty	ochrana zdraví v případě dopravní nehody

RIZIKA ZPRACOVÁNÍ

Jako každé zpracování osobních údajů nese i používání ONI systemu určitá rizika pro práva a svobody subjektů údajů, tedy zejména klientů či zaměstnanců zákazníka. Jedním ze stěžejních principů Nařízení je přístup založený na riziku, který znamená, že správce (tedy zákazník) 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 ONI systemu mohou například být:

Hrozba	**Příklad hrozby (pro ONI system)**	**Protiopatření**
Zpracování nepřesných osobních údajů	V systému jsou neaktualizované osobní údaje	Ve smlouvách o zpracování osobních údajů je obsaženo ujednání, že zákazník je povinen hlásit neprodleně provozovateli veškeré chybné, opravené, aktualizované nebo vymazané osobní údaje.
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 zákazníka pouze za účelem poskytování služby. U provozovatele je organizačně odděleno zpracování osobních údajů a obchodní a marketingové činnosti. Provozovatel zpracovává osobní údaje klientů a zaměstnanců zákazníka pouze na základě smlouvy se zákazníkem, 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 zákazníků 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 technologického centra provozovatele
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 zaměstnanců provozovatele. Logování činností zaměstnanců provozovatele.
Nadměrné sledování Porušení soukromí	ONI system je používá zákazníkem extenzivním způsobem ke sledování osob	Je povinností zákazníka zamezit použití ONI systemu extenzivním způsobem.

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

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

Správce (tedy zákazník) je povinen přijmout účinná opatření proti riziku ztráty či krádeže osobních údajů nebo zneužití přístupu k nim v těch částech ONI systemu, které jsou pod jeho kontrolou, zejména zajistit bezpečnost a omezení přístupu k je výpočetní technice a mobilním zařízením zapojeným do ONI systemu, 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 ONI systemu.

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

TECHNICKÁ A ORGANIZA ČNÍ OPATŘENÍ PROVOZOVATELE K ZABEZPEČENÍ ZPRACOVÁNÍ OSO BNÍCH ÚDAJŮ V SOULADU S POŽADAVKY NAŘÍZENÍ A ZAJIŠTĚNÍ OCHRANY PRÁV SUBJEKT U 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 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 zákazníků 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.

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

7. S výjimkou odstavce 8. níže přestane provozovatel po ukončení smlouvy se zákazníkem zpracovávat osobní údaje zpracovávané jménem zákazníka. Na základě písemného pokynu zákazníka dále provozovatel zajistí na náklady zákazníka vrácení zákazníkovi veškerých osobních údajů společně, které drží. Nepředloží-li zákazník pokyn k vrácení do dvou (2) měsíců ode dne ukončení smlouvy o zpracování osobních údajů, 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 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 dovoleného právními předpisy EU nebo členského státu, a ne pro jakýkoli jiný účel.
9. Zpracovatel jmenoval pověřence pro ochranu osobních údajů podle článku 37 Nařízení. Kontaktní údaje pověřence jsou uvedeny na www.nam.cz/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 – ONI system
2) Technická a organizační opatření k zabezpečení zpracování osobních údajů

Riziková matice - ONI system

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		2	2	4	0		0	**4**
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		4	4	16	1	4	4	**20**
Ztráta kontroly na osobními údaji		3	3	9	1	3	3	**12**
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	2	4	1	2	2	**6**
Diskriminace		0		0	0		0	**0**
Nadměrné sledování		6	7	42	1	7	7	**49**
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:				**Celková míra rizika tohoto zpracování**				**91**
Rozsah "Pravděpodobnosti" od 0 (nemožné) po 10 (jisté)								
Rozsah "Závažnosti" od 0 (žádná) po 10 (velmi vysoká)								

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 ONI SYSTEM

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

Technická a organizační opatření zajišťující identifikaci zákazníka 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 zákazníků);
- 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 ONI system měly přístup pouze k údajům, ke kterým mají přístupové právo. Dále provozovatel zajistil, aby tyto údaje nemohly být v serverové aplikaci ONI system 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 Private Network/virtuální soukromá síť);
- Digitální podpis;
- Bezpečnostní monitoring zákazníků;
- 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 zákazníků (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 se zákazníkem.

Opatření pro odlišení povinností ve vztahu k zákazníkovi jsou následující:

- Zaměstnanci provozovatele jsou povinni odlišovat zpracování údajů provozovatele, zákazníka a dalších zákazníků provozovatele;
- 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 DOSTUPNOST IÚDAJŮ

Provozovatel zavedl níže uvedená opatření, aby bylo zajištěno, že osobní údaje v ONI systemu 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:

- Více klientské řešení;
- Oddělení systémů v reálném čase a vyzkoušení prostředí;
- Dokumentované oddělení funkcí.
- Data zákazníků 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