

ČREPUBLIKA - OKRESNÍ SOUD VE SVITAVÁCH
správa soudu
Dimitrovova 33, 568 19 Svitavy
tel.:461 352 811, fax 461 352 837, e-mail: posta@osoud.svy.justice.cz
ID datové schránky: a6babkt

20Spr: 280 /2018

Svitavy 7.5.2018

Příloha: 1x monitorování prostor

SMĚRNICE
pro zajištění ochrany osobních údajů
při provozování kamerového systému

JUDr. Zdeněk Fric
předseda Okresního soudu ve Svitavách

ČÁST PRVNÍ

OBECNÁ USTANOVENÍ

§ 1

Úvodní ustanovení

- (1) Tato směrnice upravuje zpracování osobních údajů při provozování kamerového systému v podmínkách objektu Okresního soudu ve Svitavách (dále jen „okresní soud“). Upravuje postup při manipulaci s osobními údaji zpracovávanými v kamerovém systému od jejich vzniku, ukládání až k likvidaci.
- (2) Účelem této směrnice je stanovení zásad pro zpracování osobních údajů při provozování kamerového systému a zajištění jednotného postupu při přijímání a realizaci technicko-organizačních opatření k zajištění ochrany osobních údajů.
- (3) Cílem této směrnice je zejména
 - a) stanovit pravidla pro stanovení odpovědností jednotlivých osob a funkcí,
 - b) stanovit obsah zdokumentování užívaného kamerového systému,
 - c) evidenci zpracování a pohybu (předávání) osobních údajů,
 - c) zabránit vzniku škod nebo zneužití neoprávněným zpracováním osobních údajů kamerovým systémem,
 - d) zabezpečit dokumentační materiál pro řešení bezpečnostních incidentů,
 - e) zajistit ochranu osobních údajů před neoprávněnou manipulací nebo zneužitím.

§ 2

Rozsah působnosti

Tato směrnice je závazná pro všechny zaměstnance okresního soudu, kteří manipulují s osobními údaji v souvislosti s kamerovým systémem nebo jednotlivými prvky kamerového systému objektu. Kontrolou dodržování této směrnice je pověřen ředitel správy soudu.

ČÁST DRUHÁ

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

§ 3 Vymezení pojmů

V souladu s ustanovením § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon č. 101/2000 Sb.“)

- a) **osobním údajem** je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,
- b) **příjemcem** je každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje pro potřeby výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci; v případech veřejného pořádku a vnitřní bezpečnosti; předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů; významného hospodářského zájmu České republiky nebo Evropské unie; významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření,
- c) **správce** je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj; zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,
- d) **subjektem údajů** je fyzická osoba, k níž se osobní údaje vztahují,
- e) **zpracovatelem** je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle zákona č. 101/2000 Sb.

§ 4 Zpracování osobních údajů

- (1) Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je kromě kamerového sledování prováděn záznam pořizovaných záběrů nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.
- (2) Údaje uchovávané v záznamovém zařízení, ať obrazové nebo zvukové, jsou osobními údaji za předpokladu, že na základě těchto údajů lze přímo nebo nepřímo identifikovat konkrétní fyzickou osobu.

- (3) Archivační doba zpracování osobních údajů je stanovena na dobu, která je nezbytně nutná k naplnění správcem stanového účelu¹.
- (4) Po zahájení řízení v němž má záznam z kamerového systému sloužit jako důkazní prostředek se fakticky mění jeho režim a tento může být uchováván jako důkaz až do doby uplynutí lhůt k podání opravných prostředků v daném řízení.

§ 5

Účel zpracování osobních údajů

- (1) Kamerový systém instalovaný v objektu okresního soudu je provozován zejména k monitorování prostor za účelem zajištění pořádku a bezpečnosti příslušníky místní jednotky justiční stráže v souladu s ustanovením § 2 odst. 1 písm. e) zákona č. 555/1992 Sb., o Vězeňské službě a justiční strážci České republiky, ve znění pozdějších předpisů. V případě bezpečnostního incidentu mohou záznamy sloužit rovněž pro zdokumentování v přestupkovém a trestním řízení.
- (2) Snímací prvky kamerového systému, instalované na veřejném prostranství, musí být instalovány tak, aby byla snímána jen nezbytně nutná část veřejného prostranství². Jedná se především o vstupy do objektů (areálů), příjezdové nebo přístupové komunikace nebo části perimetrů budov.

ČÁST TŘETÍ

PRÁVA, POVINNOSTI A ODPOVĚDNOSTI PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V KAMEROVÉM SYSTÉMU

§ 6

Správce

- (1) Správcem ve smyslu zákona č. 101/2000 Sb. je předseda soudu.
- (2) Správce je povinen zejména
 - a) stanovit účel zpracování osobních údajů (důvod provozování kamerového systému),
 - b) stanovit prostředky zpracování osobních údajů,
 - c) stanovit způsob zpracování osobních údajů,
 - d) přijímat, provádět a dokumentovat technicko-organizační opatření k zajištění ochrany osobních údajů,

¹ Za dobu účelosti, po kterou je třeba záznam z kamerového systému dále uchovávat, případně jej předat příslušnému orgánu, který by měl zahájit nebo již zahájil řízení, jehož předmětem je prošetření činu, k jehož prokázání může záznam z kamerového systému posloužit jako důkaz, je dle stanoviska Úřadu pro ochranu osobních údajů zpravidla považována jako účelná doba záznamu sedmi dnů. Po doložení potřebných informací nelze vyloučit prodloužení účelosti doby záznamu.

² Veřejné prostranství je definováno zákonem č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů, jsou to všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky a další prostory přístupné každému bez omezení, tedy sloužící obecnímu užívání, a to bez ohledu na vlastnictví k tomuto prostoru.

- e) vést dokumentaci související s provozem kamerového systému,
 - f) při přijímání opatření podle písm. d) provádět posouzení rizik,
 - g) zajistit přístup subjektu údajů k informacím o zpracovávání jeho osobních údajů,
 - h) zajistit školení zaměstnanců, kteří při výkonu své práce zpracovávají osobní údaje,
 - i) zajistit kontrolní činnost na úseku dodržování práv a povinností při zpracování osobních údajů.
- (3) Plněním povinností podle odst. 2 je pověřen ředitel správy soudu, bezpečnostní ředitel.
- (4) Pověřením podle odst. 3 se správce nezavazuje své odpovědnosti.

§ 7

Bezpečnostní ředitel

(1) Je povinen

- a) vést v aktuálním stavu technickou dokumentaci instalovaného kamerového systému,
- b) vést v aktuálním stavu zdokumentování technicko-organizačních opatření k zajištění ochrany zpracování osobních údajů v kamerovém systému,
- c) vést v aktuálním stavu směrnici k zajištění ochrany zpracování osobních údajů v kamerovém systému,
- d) při přijímání opatření podle písm. b) a c) provádět posouzení rizik,
- e) zajistit kontrolu funkčnosti kamerového systému, v případě zjištění závady neprodleně zajistit servisní zásah dodavatele nebo servisní firmy,
- f) zajistit metodickou činnost všem uživatelům kamerového systému,
- g) zajistit dohled nad zaměstnanci provádějícími opravy nebo jiný servis kamerového systému (osobně nebo pověřením velitele místní jednotky justiční stráže),
- h) na vyžádání podávat informace oprávněným subjektům údajů a to pouze v takovém rozsahu, aby nedošlo k neoprávněnému nakládání s osobními údaji třetích osob.

(2) Je oprávněn

- a) vstupovat kdykoliv do všech prostor, kde jsou instalovány části kamerového systému,
- b) provádět kontrolu výkonu činností uživatelů kamerového systému a užívat kamerový systém,

- c) přijímat opatření k zajištění ochrany zpracování osobních údajů a opatření na zvýšení bezpečnosti zpracování,
- d) pro odstranění technických poruch a nedostatků oslovit dodavatelskou případně servisní firmu,
- e) provádět výdej (export) zpracovávaných osobních údajů správním orgánům, včetně orgánů činných v trestním nebo přestupkovém řízení nebo při řešení správních deliktů, po odsouhlasení předsedou soudu,
- f) účinně spolupracovat se všemi orgány státní správy a samosprávy k zajištění povinnosti ochrany majetku a veřejného pořádku.

§ 8

Velitel místní jednotky justiční stráže

- (1) V průběhu výkonu služby zajišťuje dohled na pracovišti nad dodržováním této směrnice.
- (2) Eviduje hlášené poruchy kamerového systému, připomínky a sdělené informace k funkčnosti kamerového systému.
- (3) Při ukončení směny zajišťuje v případě zjištěných poruch a připomínek k funkčnosti kamerového systému předání poznatků a informací hlášením řediteli správy soudu.
- (4) Na vyžádání ředitele správy soudu osobně zajišťuje dohled nad zaměstnanci provádějícími opravy nebo jiný servis kamerového systému.
- (5) Je oprávněn vytvořit v odůvodněných případech a na základě pověření bezpečnostního ředitele soudu nebo předsedy soudu kopii záznamu z kamerového systému na externí médium.

§ 9

Ostatní zaměstnanci a příslušníci místní jednotky justiční stráže

Jsou povinni zejména

- a) namátkově kontrolovat (pokud to situace a způsob instalace umožňuje) instalované prvky kamerového systému,
- b) neprodleně hlásit prostřednictvím velitele místní jednotky justiční stráže jakékoliv poškození prvků kamerového systému, zjištěné zneužití nebo poškození jednotlivých prvků nebo informací v systému,
- c) v případě zjištění poškozování nebo zneužití prvků kamerového systému neprodleně adekvátně zakročit a zajistit tak ochranu majetku a prvků kamerového systému.

§ 10

Pracovníci provádějící opravy nebo servis kamerového systému

Jsou povinni zejména

- a) provádět opravy nebo servis kamerového systému pouze na vyžádání ředitele správy soudu,
- b) provádět opravy nebo servis kamerového systému pouze pod dohledem ředitele správy soudu nebo velitele místní jednotky justiční stráže.

§ 11

Externí média

- (1) Vytvořit kopii záznamu z kamerového systému na externí médium je oprávněn velitel nebo zástupce velitele místní jednotky justiční stráže, a to na základě pověření ředitele správy soudu nebo předsedy soudu.
- (2) Po vytvoření kopie záznamu z kamerového systému na externí médium velitel nebo zástupce velitele místní jednotky justiční stráže neprodleně předá toto externí médium řediteli správy soudu, případně předsedovi soudu.
- (3) Externí média, která obsahují osobní údaje pocházející z kamerového systému (záznamy pořízené kamerovým systémem) mohou být ukládána pouze v úschovném objektu (uzamykatelná skříň, trezor apod.) umístěném v místnosti č. 462.
- (4) S těmito záznamovými médii mohou nakládat pouze ředitel správy soudu a předseda soudu.
- (5) V případě potřeby a na základě svolení předsedy soudu je možno provádět výdej (export) zpracovávaných osobních údajů správním orgánům, včetně orgánů činných v trestním nebo přestupkovém řízení nebo při řešení správních deliktů.
- (6) Výdej podle odstavce (5) je prováděn protokolárně ředitelem správy soudu, případně předsedou soudu.
- (7) Protokol o předání osobních údajů musí obsahovat klauzuli o zajištění likvidace (znehodnocení) osobních údajů po uplynutí doby potřebné k jejich deklarovanému využití.

§ 12

Povinnost mlčenlivosti

- (1) Všichni zaměstnanci okresního soudu, příslušníci místní jednotky justiční stráže a případně jiné fyzické osoby, které se podílejí na zpracování osobních údajů a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

- (2) Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.
- (3) Ustanovením předchozích odstavců není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů³.
- (4) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů⁴.

§ 13

Oznamovací a informační povinnost

- (1) Správce je povinen provést oznamovací povinnost u Úřadu pro ochranu osobních údajů.
- (2) Správce je povinen vhodným způsobem zajistit informovanost subjektů údajů, o nichž ví, že budou do monitorovaných prostor přicházet, a že do nich budou přicházet pravidelně (např. zaměstnanci správce, stálé dodavatelské firmy). Vůči těmto subjektům splní správce informační povinnost předem a v plném rozsahu (např. formou interního sdělení, se kterým budou subjekty údajů prokazatelně seznámeny).
- (3) Správce je povinen vhodným způsobem zajistit informovanost subjektů údajů, jenž budou do monitorovaných prostor přicházet nepředvídatelně a nahodile, a to alespoň v zákoně stanoveném minimálním rozsahu⁵. Zároveň subjektu údajů musí být umožněno využít jeho práva v plném rozsahu.

§ 14

Poskytování informací subjektům údajů

- (1) Každý subjekt údajů má právo získat informace o zpracování osobních údajů v rozsahu
 - a) kde a kým jsou osobní údaje zpracovávány,
 - b) kdo je odpovědný za zpřístupnění informací,
 - c) jaké osobní údaje jsou zpracovávány a za jakým účelem.
- (2) Zpřístupněny mohou být pouze takové informace a osobní údaje, které neohroží ochranu zpracovávaných osobních údajů.

³ Zvláštními zákony mohou být chápány např. zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, apod.

⁴ Např. § 167 a 168 zákona č. 140/1961 Sb., trestní zákon apod.

⁵ Pokud k obvyklému provedení splnění informační povinnosti dle § 11 resp. § 21 (např. umístění informačních cedulí) bude mít zamítavé stanovisko jiný orgán státní správy či samosprávy (např. místně příslušný památkový ústav), odkazuje Úřad pro ochranu osobních údajů na možnost správního řízení, které by směřovalo ke změně tohoto stanoviska nebo k dohodě o přijatelné formě splnění informační povinnosti (např. na přijatelné formě vzhledu a umístění informačních cedulí). Jestliže však tato změna stanoviska nebude možná, nezbyvá než se pokusit o nalezení jiného vhodného řešení (např. instalace na vstupní dveře/bránu, okna, příp. na sloupek před vstupem do monitorovaného prostoru apod.).

- (3) Nesmí být zveřejněny informace o technicko-organizačních opatřeních nebo takové informace, které by tato opatření ohrozily.
- (4) Za poskytnutí informací dle odstavce (1) je odpovědná ředitel správy soudu.
- (5) Poskytnutí informací a důvod poskytnutí informací musí být ředitelem správy soudu evidováno.

ČÁST ČTVRTÁ

TECHNICKO-ORGANIZAČNÍ OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ V KAMEROVÉM SYSTÉMU

Správce je povinen přijímat a provádět technicko-organizační opatření k zajištění ochrany osobních údajů při provozování kamerového systému.

Těmito opatřeními jsou zejména

- a) fyzická ochrana zařízení,
- b) režimová opatření.

§ 15

Fyzická ochrana zařízení

- (1) Veškerá zařízení kamerového systému a média s archivovanými osobními údaji musí být mechanicky nebo elektronicky zabezpečena proti neoprávněnému použití nebo poškození.
- (2) Vstup do místnosti se záznamovým zařízením mají pouze předseda soudu, ředitel správy soudu a příslušníci místní jednotky justiční stráže nebo osoby v jejich doprovodu, a to po schválení předsedou soudu nebo ředitelem správy soudu.
- (3) Za zajištění ochrany a funkčnosti mechanických nebo elektronických zabezpečení je odpovědný ředitel správy soudu.
- (4) Každý zaměstnanec okresního soudu nebo příslušník místní jednotky justiční stráže je povinen účinně chránit jednotlivé části kamerového systému. V případě zjištění poškození nebo nebezpečí poškození je povinen přijmout taková opatření, aby nedošlo k dalšímu poškození nebo zneužívání částí kamerového systému. O této skutečnosti je povinen neprodleně informovat ředitele správy soudu buď přímo nebo prostřednictvím velitele místní jednotky justiční stráže.

§ 16

Režimová opatření

- (1) Místnost se záznamovým zařízením je režimovým pracovištěm. Do těchto prostor mohou volně vstupovat pouze předseda soudu, ředitel správy soudu a příslušníci místní jednotky justiční stráže.

- (2) Klíče (a také příslušná oprávnění do zabezpečovacího systému) od místnosti se záznamovým zařízením mohou použít pouze příslušníci místní jednotky justiční stráže. Vstup do místnosti se záznamovým zařízením musí být velitelem místní jednotky justiční stráže evidován (předseda soudu, ředitel správy soudu a příslušníci místní jednotky justiční stráže se evidovat nemusí).
- (3) Zpracovávané osobní údaje kamerovým systémem jsou v případě potřeby vydávány (exportovány) správním orgánům včetně orgánů činných v trestním nebo přestupkovém řízení nebo při řešení správních deliktů formou protokolárního předání a po odsouhlasení předsedou soudu. Likvidaci takto předaných záznamů provádí subjekt, který je protokolárně převzal.

§ 17

Školení zaměstnanců a příslušníků místní jednotky justiční stráže

- (1) Zaměstnanci soudu a příslušníci místní jednotky justiční stráže jsou povinni účastnit se školení k obsluze kamerového systému a o způsobu a postupech ochrany osobních údajů v kamerovém systému a to v rozsahu potřebném k výkonu svých funkcí.
- (2) Provádět školení v jednotlivých stupních jsou oprávněni
 - a) u vstupního školení bezpečnostní ředitel soudu ve spolupráci s velitelem místní jednotky justiční stráže,
 - b) u opakovaného školení bezpečnostní ředitel ve spolupráci s velitelem místní jednotky justiční stráže (minimálně jednou za 2 roky).

§ 18

Dokumentace

Seznam dokumentace provozovaného kamerového systému

- a) dokumentace kamerového systému,
- b) provozní dokumentace (evidence závad, oprav a revizí kamerového systému),
- c) zdokumentování technicko-organizačních opatření k zajištění ochrany zpracování osobních údajů,
- d) směrnice k zajištění ochrany zpracování osobních údajů v kamerovém systému,
- e) evidence výdeje (exportu) osobních údajů zpracovávaných kamerovým systémem.

§ 19
Kontrolní činnost

- (1) Kontrolní činnost je prováděna bezpečnostním ředitelem.
- (2) O provedené kontrole (pravidelné i namátkové) musí být sepsán zápis, včetně informace o způsobu odstranění zjištěných nedostatků.
- (3) Kontrola systému, prověření funkčnosti a ověření stavu systému, včetně stavu ochrany osobních údajů, bude provedena minimálně jednou ročně.

ČÁST PÁTÁ

ZÁVĚREČNÁ USTANOVENÍ

§ 20
Postup při zjištění neoprávněného nakládání s osobními údaji

- (1) Při zjištění neoprávněného nakládání s osobními údaji, jakož i při zjištění jiných porušení povinností stanovených zákonem č. 101/2000 Sb., je osoba, která toto porušení zjistí, povinna neprodleně informovat ředitele správy soudu.
- (2) Bezpečnostní ředitel stanoví dle závažnosti situace postup jejího řešení v souladu s právními předpisy.

§ 21
Sankce

- (1) Porušení povinností stanovených tímto předpisem může být považováno za hrubé porušení pracovní kázně a může být postihováno dle ustanovení zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
- (2) Porušení povinností stanovených tímto pokynem příslušníky místní jednotky justiční stráže může být považováno za spáchání kázeňského přestupku a předáno k řešení příslušnému služebnímu funkcionáři Vězeňské služby České republiky.

§ 22
Účinnost

Tento pokyn nabývá účinnosti dne 26.5.2018.

JUDr. Zdeněk Fric
předseda Okresního soudu ve Svitavách