
Směrnice
„Ochrana osobních údajů v kamerovém
systému“
SAFETY PRO s.r.o.

OBSAH

1	Úvod.....	5
1.1	Úvodní ustanovení	5
1.2	Účel instalace kamerového systému	5
1.3	Správce kamerového systému	5
1.4	Informace o monitoringu.....	5
2	Specifikace kamerového systému	7
2.1	Záznamové zařízení.....	7
2.2	Monitorování záběrů.....	7
2.3	Kamery.....	7
3	Povinnosti osob oprávněných k exportu uložených dat	9
3.1	Správce kamerového systému	9
3.2	Starosta obce	Chyba! Záložka není definována.
4	Přijatá technicko-organizační opatření k zajištění ochrany osobních údajů	11
4.1	Opatření fyzické bezpečnosti	11
4.1.1	Záznamové zařízení.....	11
4.1.2	Kamery	11
4.1.3	Přenosové trasy	11
4.2	Přístup k záznamům z kamerového systému	11
5	Vzory.....	13

5.1	Informační tabulka.....	Chyba! Zázločka není definována.
5.2	Předávací protokol	13

SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

GDPR	Nařízení evropského parlamentu a rady (EU) č. 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) (General Data Protection Regulation)
Osobní údaj	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě. U kamerového systému jde zejména o podobu osoby a obrazové informace o jejím pohybu nebo jednání.
Správce	Subjekt, který určuje účely a prostředky zpracování osobních údajů. Pro účely této směrnice je správcem SAFETY PRO s.r.o., IČ: 28571690
Správce kamerového systému	Jednatel společnosti písemně určená osoba odpovědná za provoz, kontrolu funkčnosti, oprávněné nahlížení a případný export záznamů.
Subjekt údajů	Fyzická osoba, k níž se osobní údaje vztahují
Vedení společnosti	Jednatel společnosti a jím pověřené vedoucí osoby v rozsahu jejich pověření.
Zaměstnanec	Zaměstnanec společnosti nebo osoba vykonávající práci na základě dohody o práci konané mimo pracovní poměr.
Zpracování osobních údajů	Jakákoli operace s osobními údaji, zejména pořízení, uložení, vyhledání, nahlédnutí, export, předání, omezení, výmaz nebo zničení.
Bezpečnostní incident	Událost související s ochranou majetku, života nebo zdraví, podezřením na protiprávní jednání, vandalismus, neoprávněný vstup nebo jinou událost odpovídající účelu kamerového systému.
Export záznamu	Vytvoření samostatné kopie části kamerového záznamu za účelem řešení konkrétního incidentu nebo předání oprávněnému příjemci.

PREAMBULE

Názvy rolí v této směrnici jsou používány v gramatickém mužském rodě pouze pro zjednodušení textu. Ustanovení se použijí shodně bez ohledu na pohlaví osoby, která danou roli vykonává.

Směrnice vychází z obecného nařízení GDPR, zákona č. 110/2019 Sb., o zpracování osobních údajů, a z principů aktuální metodiky Úřadu pro ochranu osobních údajů ke kamerovým systémům

1 ÚVOD

1.1 ÚVODNÍ USTANOVENÍ

Tato Směrnice k ochraně osobních údajů v kamerovém systému (dále jen „směrnice“) stanovuje pravidla pro zpracování a ochranu osobních údajů prostřednictvím kamerového systému provozovaného společností SAFETY PRO s.r.o. (dále jen „společnost“).

Směrnice se vztahuje na kamerový systém se záznamem instalovaný po obvodu budovy společnosti. Monitorování je omezeno na soukromý pozemek objektu; zóny záznamu mají být nastaveny tak, aby nezabíraly veřejný prostor ani sousední nemovitosti nad rozsah nezbytný pro ochranu areálu.

Kamerový systém pořizuje pouze obrazový záznam. Zvukový záznam, biometrická identifikace, rozpoznávání obličejů ani automatizované rozhodování nejsou používány.

1.2 ÚČEL INSTALACE KAMEROVÉHO SYSTÉMU

Účelem kamerového systému je ochrana majetku společnosti, ochrana života a zdraví osob nacházejících se v areálu, prevence vandalismu a neoprávněných vstupů a pořízení podkladů pro objasnění a prokázání konkrétních bezpečnostních incidentů.

Právním základem zpracování je čl. 6 odst. 1 písm. f) GDPR – oprávněný zájem společnosti na ochraně majetku a osob. Společnost musí tento oprávněný zájem a nezbytnost konkrétního nastavení kamerového systému doložit dokumentovaným balančním testem.

Záznamy lze zpřístupnit pouze v odůvodněných případech, zejména orgánům činným v trestním řízení, správním orgánům, soudům, pojišťovně nebo jiné osobě, pokud je takové zpřístupnění nezbytné pro řešení incidentu nebo ochranu právních nároků

1.3 SPRÁVCE KAMEROVÉHO SYSTÉMU

Správcem osobních údajů je SAFETY PRO s.r.o. Správcem kamerového systému ve smyslu této interní směrnice je jednatelem určená osoba.

Správce kamerového systému má přístup k online obrazu a uloženým záznamům pouze v rozsahu potřebném pro výkon své role a za podmínek této směrnice.

1.4 INFORMACE O MONITORINGU

Osoby vstupující do monitorovaného prostoru musí být ještě před vstupem do záběru kamer informovány viditelnou informační tabulkou. Vzor tabulky je uveden v čl. 5.1 této směrnice.

Informační tabulka obsahuje alespoň:

- a)** sdělení, že prostor je monitorován kamerovým systémem se záznamem a piktogram kamery;
- b)** identifikaci správce – SAFETY PRO s.r.o., IČO 28571690;
- c)** hlavní účel zpracování a informaci o právním základu – oprávněný zájem;
- d)** základní informaci o době uchování a kontaktní místo, kde lze získat úplné informace podle čl. 13 GDPR.

Úplné informace o zpracování musí být dostupné v sídle společnosti a dále prostřednictvím: <https://www.safetypro.cz/> , hronkova@safetypro.cz, + 420 734 712 033, . Zaměstnanci musí být o rozsahu a způsobu monitorování předem informováni přímo; kamerový systém nesmí být používán k soustavné kontrole jejich pracovního výkonu.

Na žádost subjektu údajů společnost poskytne zejména informace o:

- identitě a kontaktních údajích správce;
- účelech zpracování, oprávněném zájmu a rozsahu snímaného prostoru;
- kategoriích osobních údajů – obrazový záznam bez zvuku;
- místě zpracování, době uchování a způsobu automatického přepisu záznamů;
- příjemcích nebo kategoriích příjemců záznamu;
- právech subjektu údajů a možnosti podat stížnost u Úřadu pro ochranu osobních údajů.

Subjekt údajů může podle podmínek GDPR zejména uplatnit právo na přístup, výmaz nebo omezení zpracování a právo vznést námitku proti zpracování založenému na oprávněném zájmu. Technická povaha záznamu může ovlivnit způsob, jakým lze jednotlivá práva realizovat, zejména pokud nelze osobu nebo konkrétní časový úsek spolehlivě identifikovat.

Žádosti týkající se kamerových záznamů musí být vyřízeny bez zbytečného odkladu a v zákonných lhůtách. Při poskytnutí kopie záznamu musí být chráněna práva a svobody dalších zachycených osob, například anonymizací nebo jiným vhodným opatřením.

2 SPECIFIKACE KAMEROVÉHO SYSTÉMU

2.1 ZÁZNAMOVÉ ZAŘÍZENÍ

Záznamové zařízení: HikVision DS-7018HGHI (označení dle informace společnosti). Zařízení je umístěno v uzamčené budově, v kanceláři správce kamerového systému.

Přístup k zařízení a k uloženému obrazu je chráněn bezpečným heslem. Obraz a záznam může standardně sledovat pouze správce kamerového systému na monitoru v kanceláři správce.

Doba běžného uchování obrazového záznamu je nastavena na maximálně 30 dnů. Po uplynutí této doby jsou záznamy automaticky přepisovány novými záznamy, nebyly-li v souladu s účelem této směrnice odděleně exportovány jako záznam konkrétního incidentu.

Záznam konkrétního incidentu lze po odděleném exportu uchovávat po dobu nezbytnou pro jeho projednání, pro uplatnění nebo obhajobu právních nároků, pro pojistnou událost nebo pro řízení před příslušným orgánem. Po pominutí účelu se taková kopie bezpečně vymaže.

2.2 MONITOROVÁNÍ ZÁBĚRŮ

Stálé aktivní sledování osob není účelem systému. Online obraz a uložené záznamy smí správce kamerového systému využívat pouze pro ochranu areálu, řešení konkrétního incidentu, ověření funkčnosti nebo další činnost výslovně dovolenou touto směrnicí.

Vzdálené sledování mimo monitor v kanceláři správce není touto směrnicí povoleno, pokud nebude samostatně schváleno jednatelem, technicky zabezpečeno a promítnuto do této směrnice a související dokumentace.

2.3 KAMERY

Umístění	Po obvodu budovy / objektu společnosti.
Zorné pole	Soukromý pozemek objektu. Zóny záznamu jsou nastaveny tak, aby snímaly pouze pozemek objektu; veřejný prostor a sousední nemovitosti nemají být cíleně monitorovány.
Typ	HikVision DS-2CD21DC.
Záznam	Pouze obrazový záznam; zvuk se nenahrává.
Režim záznamu	kontinuální
Doba uložení	Maximálně 30 dnů; po uplynutí doby automatický přepis, s výjimkou exportu konkrétního incidentu.
Účel	Ochrana majetku a osob, prevence a dokumentace bezpečnostních incidentů, zajištění důkazního materiálu při podezření na protiprávní jednání.
Zakázané použití	Soustavná kontrola pracovního výkonu zaměstnanců, pořizování zvuku, biometrické rozpoznávání a jiné použití nesouvisející s deklarovaným účelem.

Technická dokumentace nebo situační plán kamer musí umožnit jednoznačně přiřadit jednotlivé kamery k jejich fyzickému umístění a zornému poli. Při změně polohy, počtu kamer nebo záběru se dokumentace aktualizuje před uvedením změny do běžného provozu.

Pokud se ukáže, že kamera zasahuje mimo soukromý pozemek více, než je nezbytné, správce kamerového systému zajistí úpravu směru, zorného pole nebo vhodné maskování obrazu

3 POVINNOSTI OSOB OPRÁVNĚNÝCH K EXPORTU ULOŽENÝCH DAT

3.1 SPRÁVCE KAMEROVÉHO SYSTÉMU

- 1) Zachovávat mlčenlivost o osobních údajích zpracovávaných kamerovým systémem a o bezpečnostních opatřeních k jejich ochraně, a to i po skončení pověření.
- 2) Zajistit, aby informační tabulky byly umístěny před vstupem do monitorovaného prostoru, byly čitelné a odpovídaly aktuálnímu nastavení systému.
- 3) Zajišťovat provozuschopnost kamerového systému. Při servisním zásahu umožnit technikovi přístup pouze v nezbytném rozsahu a po dobu zásahu zajistit dohled, pokud by mohl přijít do styku se záznamy.
- 4) Chránit přístupové heslo; nesdílet jej s neoprávněnými osobami, nepoužívat stejné heslo pro jiné služby a bezodkladně jej změnit při podezření na kompromitaci.
- 5) Nahlížet do uložených záznamů pouze tehdy, je-li to nezbytné pro konkrétní účel podle této směrnice, pro ověření funkčnosti nebo pro vyřízení řádně uplatněného práva subjektu údajů.
- 6) Exportovat záznam pouze v souvislosti s konkrétním incidentem, na pokyn nebo s vědomím jednatele společnosti, případně na základě řádné žádosti oprávněného orgánu. O exportu pořídít záznam v provozní knize.
- 7) Při předání exportu externímu příjemci vyhotovit předávací protokol podle čl. 5.2 a evidovat datum, důvod, časový rozsah, zdrojovou kameru, příjemce a osobu, která předání provedla.
- 8) Vést provozní knihu kamerového systému. Evidovat zejména poruchy, změny nastavení, servisní zásahy, nahlížení související s incidentem, exporty, předání záznamů a bezpečnostní události.
- 9) Nejméně jednou za 6 měsíců provést kontrolu funkčnosti systému a ověřit správné přepisování záznamů; zkušebně vytvořená data bezprostředně po ověření odstranit a kontrolu zapsat do provozní knihy
- 10) Bezodkladně oznámit jednateři každé podezření na neoprávněný přístup, ztrátu exportovaného záznamu, porušení zabezpečení nebo jiný incident ochrany osobních údajů.
- 11) Předat kontaktní osobě pro ochranu osobních údajů každou žádost subjektu údajů, kterou nelze vyřídit čistě technicky v rámci předem stanoveného postupu.

3.2 JEDNATEL SPOLEČNOSTI

- 1) Určuje správce kamerového systému a případné další oprávněné osoby. Každé oprávnění musí být omezeno na nezbytný rozsah a pravidelně přezkoumáváno.
- 2) Zajišťuje, aby kamerový systém měl dokumentovaný oprávněný zájem, bilanční test, záznam o činnosti zpracování a aktuální informační povinnost podle čl. 13 GDPR.
- 3) Před schválením 30denní doby uchování posoudí a dokumentuje konkrétní důvody, které tuto dobu činí nezbytnou; není-li nezbytnost doložena, rozhodne o zkrácení doby uchování.
- 4) Rozhoduje o předání záznamu třetím osobám a o delším uchování exportu konkrétního incidentu, není-li takové rozhodnutí dáno přímo zákonnou povinností nebo závazným požadavkem orgánu veřejné moci.
- 5) Zajišťuje pravidelný přezkum této směrnice, zejména při změně technologie, počtu kamer, zorného pole, doby uchování, režimu přístupu nebo účelu zpracování.

4 PŘIJATÁ TECHNICKO-ORGANIZAČNÍ OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

4.1 OPATŘENÍ FYZICKÉ BEZPEČNOSTI

4.1.1 ZÁZNAMOVÉ ZAŘÍZENÍ

Záznamové zařízení HikVision DS-7018HGHI je umístěno v kanceláři správce kamerového systému v uzamčené budově.

Přijatá opatření:

- 1) Místnost se záznamovým zařízením musí být mimo dobu oprávněné přítomnosti uzamčena. Přístup do místnosti mají pouze osoby, jejichž přístup je nezbytný pro výkon pracovních povinností.
- 2) Záznamové zařízení a rozhraní pro sledování obrazu jsou chráněny bezpečným heslem. Heslo má znát pouze oprávněná osoba; sdílené obecné účty se nepoužívají, pokud zařízení umožňuje individuální účty.
- 3) Monitor nesmí být umístěn tak, aby na obraz běžně viděly neoprávněné osoby. Při opuštění pracoviště se přístup k zařízení uzamkne nebo odhlásí.

4.1.2 KAMERY

Přijatá opatření:

- 1) Kamery jsou umístěny po obvodu budovy a jejich záběry jsou omezeny na soukromý pozemek objektu.
- 2) Kamery musí být umístěny nebo chráněny tak, aby byla přiměřeně omezena možnost neoprávněné manipulace, změny směru nebo poškození.
- 3) Při údržbě se vždy ověří, že nedošlo k rozšíření zorného pole mimo nezbytný rozsah.

4.1.3 PŘENOSOVÉ TRASY

Přenosové trasy a síťové prvky kamerového systému musí být fyzicky a logicky chráněny proti neoprávněnému přístupu. Jejich konkrétní provedení se vede v technické dokumentaci systému. Změny, které umožní vzdálený přístup nebo cloudové ukládání, vyžadují předchozí posouzení rizik a aktualizaci této směrnice.

4.2 PŘÍSTUP K ZÁZNAMŮM Z KAMEROVÉHO SYSTÉMU

Přijatá opatření:

- 1) Instalace a nastavení kamer respektují právo na soukromý a osobní život. Systém je zaměřen na ochranu soukromého pozemku a nesmí být používán k cílenému sledování sousedních nemovitostí, veřejných komunikací nebo jiných prostor bez samostatného právního posouzení.
- 2) Standardní přístup k online obrazu a uloženým záznamům má pouze správce kamerového systému prostřednictvím heslem chráněného zařízení v jeho kanceláři.

-
- 3) Případná další oprávněná osoba musí být určena jednatelem a má mít, pokud to zařízení umožňuje, vlastní přístupové údaje. Přístup se odebere bezodkladně po zániku důvodu oprávnění.
 - 4) Export záznamu je přípustný pouze při řešení konkrétního bezpečnostního incidentu, pro ochranu právních nároků, pro vyřízení práva subjektu údajů nebo na základě oprávněného požadavku příslušného orgánu.
 - 5) Exportovaný soubor se ukládá na zabezpečené médium nebo úložiště s omezeným přístupem. Kopie se nevytvářejí nad nezbytný počet a po pominutí účelu se nevratně odstraní.
 - 6) Předání záznamu externímu příjemci musí být prokazatelné. Použije se předávací protokol a zaznamená se rozsah předaných údajů a důvod předání.
 - 7) Přístupy, exporty a servisní zásahy se evidují v provozní knize; pokud zařízení umožňuje systémové logování, logy se pravidelně kontrolují a chrání před neoprávněnými změnami.
 - 8) Servisní organizace nesmí bez právního důvodu pořizovat kopie záznamu. Pokud servis vyžaduje přístup k osobním údajům, musí být právní role servisního dodavatele předem posouzena a případně upravena smluvně podle GDPR.
 - 9) Každá změna kamerového systému, která významně zvyšuje rozsah nebo intenzitu monitoringu, se předem posoudí z hlediska nezbytnosti, proporcionality a případné potřeby posouzení vlivu na ochranu osobních údajů (DPIA).

5 VZORY

5.1 PŘEDÁVACÍ PROTOKOL

Předávací protokol

Důvod předání média / souboru se záznamem kamerového systému:

.....
.....
.....

Rozsah předávaných osobních údajů (časový úsek, označení kamery, název souboru, případně další identifikace):

.....
.....
.....

Příjemce záznamu (orgán / organizace / osoba, identifikace žádosti nebo spisu):

.....
.....

Předáno dne:

.....
Předal

(funkce, jméno, příjmení, podpis)

.....
Převzal

(funkce, jméno, příjmení, podpis)

Poznámka: Předání musí být evidováno také v provozní knize kamerového systému. Uveďte konkrétní důvod (např. poškození či krádež majetku společnosti, pojistná událost, žádost Policie ČR s identifikací věci apod.).

Ochrana kopie: Exportovaný záznam se uchovává pouze po dobu nezbytnou k vyřízení konkrétního případu a poté se bezpečně odstraní, není-li další uchování vyžadováno právním předpisem nebo probíhajícím řízením.