

<https://doi.org/10.5817/RPT2025-2-5>

ZÁZNAMY UDÁLOSTÍ: STANOVENÍ DOBY UCHOVÁNÍ A IMPLEMENTACE KOMPLEXNÍCH POŽADAVKŮ V ORGANIZACI¹

JAKUB SAUER,² STANISLAV ŠPAČEK,³ PATRIK FRÁŇA,⁴ DENISA
DRAPPANOVÁ⁵ A JAKUB HARAŠTA⁶

ABSTRAKT

Security Information and Event Management (SIEM) jsou standardní součástí infrastruktury řady organizací. Jde o nástroje sloužící k monitoringu provozu systémů a sítí, korelaci událostí a uchování těchto údajů pro jejich pozdější využití. Jde o způsob, jakým je možné shromažďovat a konsolidovat záznamy události a další relevantní informace z různých zdrojů. V principu SIEM umožňuje pružnější reakci na kybernetické události a incidenty, ale přispívá také k efektivnější správě provozovaných systémů a sítí.

¹ Vznik publikace byl podpořen projektem specifického výzkumu Právo a technologie XIII (MUNI/A/1739/2024, Denisa Drappanová) a projektem Grantové agentury MU Forensic Support for Building Trust in Smart Software Ecosystems (MUNI/G/1142/2022, Jakub Harašta). Názory uvedené v příspěvku nevyjadřují oficiální postoj organizací, ke kterým jsou jednotliví autoři afiliováni.

² Mgr. Jakub Sauer je IT specialista působící na Ústavu výpočetní techniky Masarykovy univerzity. Kontaktní e-mail: sauer@ics.muni.cz

³ RNDr. Stanislav Špaček, Ph. D. je výzkumným a vývojovým pracovníkem na Ústavu výpočetní techniky Masarykovy univerzity. Kontaktní e-mail: spaceks@ics.muni.cz.

⁴ Mgr. Patrik Fráňa je referentem Národního úřadu pro kybernetickou a informační bezpečnost. Kontaktní e-mail: PatrikFrana@seznam.cz.

⁵ Mgr. Denisa Drappanová je doktorandkou Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v programu Právo informačních a komunikačních technologií. Kontaktní e-mail: 493922@mail.muni.cz.

⁶ JUDr. Mgr. Jakub Harašta, Ph. D. je odborným asistentem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: harasta@muni.cz.

SIEM může organizace implementovat mimo jiné za účelem vyhovění legislativním požadavkům, které na organizaci mohou dopadat (např. povinnost monitorovat a vyhodnocovat kybernetické bezpečnostní incidenty). S tím je spojeno mnoho problematických aspektů, které mohou být obtížně identifikovatelné, a to jak IT odborníky pracujícími s uvedenými nástroji, tak právními experty, kteří si nemusí vždy nutně uvědomit složitost technologického řešení.

Článek je zaměřen na výklad a implementaci legislativních požadavků, které dopadají na SIEM způsobem umožňujícím SIEM využít s minimalizací právního rizika plynoucího z nedostatečné implementace. Cílem tohoto textu je (1) vymezit požadavky plynoucí z překrývajících se právních předpisů v oblasti kybernetické bezpečnosti, ochrany osobních údajů a elektronických komunikací, (2) identifikovat místa, kde se překrývají nebo jsou v konfliktu, a (3) navrhnout postupy k zajištění souladu SIEM s právními požadavky.

KLÍČOVÁ SLOVA

Uchování dat; záznamy bezpečnostních událostí; SIEM; compliance

ABSTRACT

Security Information and Event Management (SIEM) is a standard part of the infrastructure of many organizations. These are tools used to monitor the operation of systems and networks, to correlate events, and to store this data for later use. It is a way to collect and consolidate event logs and other relevant information from various sources. In essence, SIEM enables a more flexible response to cyber events and incidents, while also contributing to more efficient management of operated systems and networks.

Organizations may implement SIEM, among other reasons, to comply with applicable legislative requirements (e.g., the obligation to monitor and evaluate cybersecurity incidents). This involves many problematic aspects that can be difficult to identify, both for IT professionals working with these tools and for legal experts, who may not always be aware of the complexity of the technological solution.

The text focuses on interpreting and implementing legislative requirements that affect SIEM, enabling its use while minimizing the legal risk arising from in-

sufficient implementation. The aim is to (1) define the requirements arising from overlapping legislation in the areas of cybersecurity, personal data protection, and electronic communications, (2) identify areas where they overlap or are in conflict, and (3) propose procedures to ensure SIEM compliance with legal requirements.

KEYWORDS

Retention of data; Security Records, SIEM; Compliance

1. ÚVOD

Článek se zabývá problematikou uchovávání a správy bezpečnostních informací a událostí v organizaci. Jde o problematiku důležitou a komplexní nejenom z technického, ale i z právního pohledu.⁷

Text se věnuje dvěma souvisejícím výzkumným otázkám: Jaké jsou požadavky právních předpisů na stanovení doby uchování a zabezpečení záznamů událostí zpracovávaných logovacím nástrojem? Jaké jsou technické možnosti implementace právních požadavků na uchovávání údajů?

Ze záběru je zřejmé, že předložený text není a nemá být přehledem legislativy dopadajícím na problematiku. V zásadě jde o komplexní *compliance* zadání identifikující nejenom dopadající právní požadavky, ale navrhuující také jejich promítnutí do technické vrstvy.

Příspěvek je strukturován následovně: po úvodu následuje první kapitola věnující se vymezení problematiky SIEM (Security Information and Event Management). Druhá kapitola mapuje právní pravidla dopadající na problematiku zpracování událostí v SIEM. Třetí kapitola identifikuje procesy k adresování právních požadavků. Čtvrtá kapitola se pak věnuje technické implementaci identifikovaných požadavků vč. automatizace. Pátá kapitola představuje závěr textu.

⁷ Srov. MENGES, Florian, Tobias LATZO, Manfred VIELBERTH, Sabine SOBOLA, Henrich C. POHLS, Benjamin TAUBMANN, Johannes KOSTLER, Alexander PUCHTA, Felix FREILING, Hans P. REISER a Günther PERNUL. Towards GDPR-compliant data processing in modern SIEM systems, *Computers & Security*, 2021, sv. 103, 102165.

2. POVAHA A ROLE SIEM

Termín Security Information and Event Management (dále také jen „SIEM“) označuje komplexní systém pro správu bezpečnostních informací a událostí v organizaci. Jeho účelem je shromažďovat kyberbezpečnostně-relevantní data z kybernetického prostředí organizace a podpořit nebo automatizovat jejich analýzu a vyhodnocení v reálném čase.⁸ Konkrétně si lze pod tímto pojmem představit širokou škálu informací – síťový provoz, události z mezilehlých síťových prvků, serverů, služeb, i z koncových zaměstnaneckých stanic. Zjednodušeně řečeno, SIEM je systém, který shromažďuje informace ze zařízení zapojených v síti organizace a tato data filtruje, agreguje, koreluje⁹, a vyhodnocuje. V případě, že v monitorovaných datech odhalí kyberbezpečnostní událost, nebo i jen anomálii, pak buď sám provede automatizovanou reakci, nebo alespoň vygeneruje upozornění pro kyberbezpečnostní operátory. Zastřešujícím cílem všech funkcí SIEM je zajištění dostatečné úrovně kybernetické bezpečnosti v organizaci.¹⁰

Přes značné pokroky v oblasti umělé inteligence¹¹ je v centru prevence a reakce na kyberbezpečnostní incidenty stále nezbytný expertní lidský operátor. SIEM je nástrojem, který má operátorovi v zajišťování kybernetické bezpečnosti asistovat a sejmout z něj zátěž v případech, kdy je to možné. Zejména tedy slouží jako jednotný centrální systém pro přístup ke kyberbezpečnostně relevantním datům. Kde původně musel operátor data

⁸ Viz GONZÁLEZ-GRANADILLO, Gustavo, GONZÁLEZ-ZARZOSA, SUSANA and DIAZ Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. [online]. 2021, roč. 21, č. 14, [cit. 20. 9. 2025], s. 2. Viz také BHATT, Sandeep, MANADHATA, Pratyusa K. a ZOMLOT, Loai. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*. [online]. 2014, roč. 12, č. 5, [cit. 20. 9. 2025], s. 35-37.

⁹ Tzn. data sjednocuje a shrnuje z mnoha zdrojů do jednoho přehledného celku (agreguje) a hledá mezi nimi souvislosti a vztahy (koreluje).

¹⁰ VELÁSQUEZ, Juan, Miguel, Lopez, MONTERRUBIO, Sergio, Mauricio, Martínez, CRESPO, Luis, Enrique, Sánchez and ROSADO, David, Garcia. Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*. [online]. 2023, roč. 22, [cit. 20. 9. 2025], s. 692-693.

¹¹ ALI, Sijjad; WANG, Jia a LEUNG, Victor Chung Ming. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms- A comprehensive review. *Information Fusion*. [online]. 2025, svazek 118, [cit. 20. 9. 2025], s. 3-4, 10-17.

vztahující se k jednomu incidentu manuálně dohledávat až na úrovni logů jednotlivých služeb, v SIEM najde vše na jednom místě. S tím souvisí i pokročilé možnosti agregace bezpečnostních dat pocházejících z různých míst v síti do upozornění (tzv. *alertů*) vyšší úrovně, což by při lokální bezpečnostní analýze dat nebylo možné. SIEM je tak schopen použít komplexnější procesy pro identifikaci podezřelého chování v síti. V neposlední řadě pak umí SIEM automatizovat reakce na některé dobře známé a popsané útoky a řešit je v semiautonomním režimu pod dohledem operátora. Vzhledem k množství kyberbezpečnostně-relevantních dat, která vygeneruje i síť menší organizace poskytující dnes běžné služby, je SIEM kritickým kyberbezpečnostním nástrojem.¹²

Základní funkcí SIEM je shromažďování kyberbezpečnostně-relevantních dat. Na úplnosti a korektnosti těchto dat totiž stojí všechny další operace, které SIEM provádí. Monitorování by mělo pokrývat primárně všechna důležitá zařízení a služby organizace, ale i ostatní prvky, zejména mezilehlá síťová zařízení.¹³ Pod toto monitorování by měly spadat také koncové zaměstnanecké nebo uživatelské stanice. Systémem shromažďovaná data tak budou nutně zahrnovat informace o zaměstnancích, klientech, i jiných osobách, které interagovaly s infrastrukturou organizace (např. navštívily její webové stránky). Je zde tedy nutné balancovat potřebu organizace na zajištění kybernetické bezpečnosti, a zájmy osob, jichž se organizací zpracovávaná data týkají. Zásadními oblastmi, které je z pohledu práva při provozu SIEM nutné adresovat, jsou z našeho pohledu zejména retence kyberbezpečnostně-relevantních dat a řízení přístupu k nim.¹⁴

Za účelem sjednocení výše popsaných kyberbezpečnostně-relevantních dat se kterými SIEM pracuje bude pro účely tohoto článku používán pojem záznam událostí. Pod záznamem událostí si lze představit informace o udá-

¹² SASHWIN, K; NITHIKA, K S; PRIYADHARSHINI, S; MADUVANT, S P a SARANYA. Analysis, Trends, and Utilization of Security Information and Event Management (SIEM) in Critical Infrastructures. *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)*. [online]. 2024, [cit. 20. 9. 2025], s. 1980-1983.

¹³ *Ibid.*, s. 1980-1981.

¹⁴ LIU, Che-Wei; HUANG, Peng a LUCAS, Henry C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*. [online]. 2019, roč. 37, č. 3, [cit. 20. 9. 2025], s. 761-762.

lostech¹⁵ komunikačního systému nebo technického zařízení. Typicky záznamy událostí představují informace o tom, co, kdy, kde, jak a kým bylo v systému provedeno (např. přihlášení, změny konfigurace, přístup k datům, selhání systémů apod.). Záznamy událostí mohou sloužit pro účely auditu, detekce bezpečnostních incidentů, ladění systémů a zajištění souladu s právními předpisy. V souvislosti se záznamem událostí je nutné vymezit také jejich zpracování, neboť v návaznosti na to právní předpisy formulují požadavky na zabezpečení dostupnosti, důvěrnosti a integrity, či stanovení doby uchování.

Zpracování poté představuje operace nebo soubor operací, který je prováděn pomocí či bez pomoci automatizovaných postupů.¹⁶ Tyto postupy mohou být např. shromáždění, uložení nebo odstranění.¹⁷ Zpracování je přitom s ohledem na požadavky právních předpisů naprosto zásadním konceptem. Samotná informace o záznamu události (například čas, délka hovoru) nemá takovou vypovídající hodnotu pro jeho zabezpečení, či nastavení doby zpracování. Pokud je ale záznam zasazený do kontextu zpracování, je možné zjistit jeho účel a také například identifikovat rizika, před kterými je potřeba zpracování záznamu událostí zabezpečit.¹⁸ Zároveň mohou informace o zpracování záznamu událostí sloužit pro ověření, zdali dochází k dosažení stanoveného účelu pro zpracování.¹⁹

¹⁵ MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015, s. 99-101.

¹⁶ V mnoha ohledech se tato definice kryje s pojmem zpracování ve smyslu článku 4 odst. 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

¹⁷ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 32.

¹⁸ Např. narušení dostupnosti zpracování záznamu událostí v důsledku zaplavení serverovny.

¹⁹ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 132-133.

3. ZPRACOVÁNÍ ZÁZNAMŮ UDÁLOSTÍ V PROSTŘEDÍ SIEM

3.1 VYMEZENÍ RELEVANTNÍCH PRÁVNÍCH PŘEDPISŮ

Jak je uvedeno výše, zpracování záznamů událostí v prostředí SIEM může zahrnovat velmi citlivé informace o samotné organizaci i o dotčených fyzických osobách. Narušení jejich dostupnosti, důvěrnosti anebo integrity by mohlo způsobit významnou škodu organizaci, dotčeným osobám a v případě některých služeb také státu. Tento závěr lze dovést například z § 4 odst. 1 písm. a) zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“).

Zákonodárce se rozhodl regulovat jejich zpracování především skrze dále uvedené právní předpisy, jejichž požadavky tento příspěvek zpracovává. Z důvodu, že součástí záznamů událostí mohou být osobních údaje je na místě také upozornit na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „nařízení GDPR“). V poslední řadě v tomto příspěvku zohledňujeme zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „ZEK“). Tato kapitola dále shrnuje relevantní požadavky uvedených předpisů s ohledem na zpracování dat v rámci SIEM a celkový účel tohoto textu. Byť v praxi není běžné, že by na každý jeden záznam událostí dopadaly všechny uvedené právní předpisy, je cílem této práce představit i takové situace, ke kterým by mohlo teoreticky dojít. Je však namístě uvést, že článek neuvádí vyčerpávající výčet legislativy, která na zpracování záznamů událostí spadá. Další, v tomto článku nerozebírané, požadavky lze nalézt například v prováděcím nařízení Komise (EU) 2024/2690, které funguje jako obdoba prováděcích předpisů ZoKB pro vybrané regulované služby.²⁰

3.2 ZOKB

V době přípravy tohoto textu již byl schválen ZoKB, který nabyl účinnosti 1. 11. 2025. ZoKB rozděluje povinné osoby do 2 režimů povinností, které

²⁰ Viz § 18 ZoKB.

popisuje v prováděcích předpisech. Těmito jsou aktuálně vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále také jen “VNR”) a vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále také jen “VVR”).

Primárním rozdílem v otázce zaznamenávání událostí mezi původní a novou legislativou je rozdíl v době uchování záznamů událostí. Nová legislativa totiž požaduje podle § 22 odst. 5 písm. c) minimálně 18 měsíců s tím, že tato povinnost se vztahuje na poskytovatele služeb v režimu vyšších povinností.

§ 23 VVR požaduje po povinných osobách uchování bezpečnostních událostí technických aktiv (technických nebo programových prostředků) pro účely zkoumání bezpečnostních incidentů a případné spolupráce s relevantními orgány. Pokud je povinná osoba identifikována jako poskytovatel regulovaných služeb v režimu vyšších povinností, má povinnost zaznamenávat události detekované za pomoci nástroje pro detekci v rámci komunikační sítě, na síťovém perimetru a v technických aktivech. Náležitosti záznamu těchto událostí podle ZoKB a prováděcích předpisů zachycuje Tabulka 1.

| | |
|---|---|
| Náležitosti záznamu událostí ve vyšším režimu povinností | Datum a čas; typ činnosti; dotčené technické aktivum; účet původce; zařízení původce; úspěšnost činnosti. |
| Události, které se zaznamenávají ve vyšším režimu | Přihlášení; provedení a neúspěšné pokusy o provedení privilegovaných činností; manipulace a neúspěšné pokusy o manipulaci s uživatelskými účty, oprávněními a přístupovými právy; pokusy o provedení činností, které nebyly dokončeny z důvodu nedostatečných přístupových práv nebo oprávnění; zahájení a ukončení |

| | |
|---|---|
| | činností technických aktiv; kritická a chybová hlášení generovaná technickými aktivy; přístupy a neúspěšné pokusy o přístupy k záznamům událostí; manipulace a neúspěšné pokusy o manipulaci se záznamy událostí; změny a neúspěšné pokusy o změny nastavení nástrojů pro zaznamenávání událostí a další činnosti uživatelů, které mohou mít vliv na bezpečnost regulované služby. |
| Záznamy událostí v režimu nižších povinností | V souladu s § 9 VNR, požaduje zaznamenávat události zejména na serverech a koncových stanicích, přičemž o událostech požaduje zaznamenávat informace (datum; čas; typ činnosti; ...), nepředepisuje však minimální dobu uchování záznamů událostí, ani typové události, které mají být zaznamenávány. V tomto ohledu může režim vyšších povinností zároveň sloužit jako inspirace pro důkladné řešení zaznamenávání událostí i pro osoby, které spadají pouze do režimu nižších povinností. |

Tabulka 1: Náležitosti záznamu událostí podle ZoKB a prováděcích předpisů

3.3 NAŘÍZENÍ GDPR

Nařízení GDPR se zabývá ochranou osobních údajů. Jak již bylo uvedeno výše, osobní údaje jsou často součástí zpracování záznamů událostí. Podle nařízení GDPR jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou pak je podle článku 4 odst. 1 nařízení GDPR fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, identifikační číslo, lokační údaje, síťový iden-

tifikátor²¹) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Středobodem ochrany osobních údajů je jejich zpracování.²²

Zpracování osobních údajů musí probíhat na základě titulů, které jsou uvedeny v čl. 6 nařízení GDPR. Pro účely zpracování záznamů událostí lze uvažovat zejména o následujících titulech pro zpracování:

1. **Plnění právní povinnosti (čl. 6 odst. 1 písm. c) nařízení GDPR);** Tento titul je aplikovatelný, pokud zpracování vyplývá z povinností stanovených právními předpisy. V kontextu zákona o kybernetické bezpečnosti (ZoKB) a prováděcích vyhlášek jde zejména o:
 - § 13 ZoKB v povinnosti poskytovatele regulované služby zavádět a provádět bezpečnostní opatření v rozsahu stanoveném vyhláškami.
 - § 15 ZoKB v povinnosti hlásit kybernetické bezpečnostní incidenty.
 - VNR a VVR obsahují detailní požadavky na detekci, zaznamenávání a uchovávání bezpečnostních a provozních událostí (např. § 9 VNR ukládá uchovávat záznamy po dobu stanovenou na základě bezpečnostních potřeb).
2. **Oprávněný zájem (čl. 6 odst. 1 písm. f) nařízení GDPR);** Oprávněný zájem lze použít, pokud správce prokáže, že jeho zájem na zpracování převažuje nad právy subjektů údajů, typicky skrz balanční test. Musí tedy existovat oprávněný zájem sledovaný správcem (např. zajištění kybernetické bezpečnosti, prevence incidentů, ochrana majetku), pro jehož naplnění je nezbytné zpracování, protože jej není možno dosáhnout jinak. Zároveň pak musí

²¹ V kontextu tohoto článku se dále může jednat například o IP adresu, přihlašovací údaje účtů, čas a způsob přihlášení uživatele, použitý prohlížeč nebo zařízení apod.

²² Zpracováním osobních údajů je podle nařízení GDPR jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení, dle článku 4 odst. 2 nařízení GDPR.

platit, že práva subjektů údajů na nezpracování nepřevažují nad oprávněným zájmem správce.

Oprávněný zájem by se v praxi mohl objevit například při uchovávání logů pro účely interního vyšetřování bezpečnostních incidentů nebo monitoring přístupů do systémů za účelem prevence zneužití (pokud nejde o realizaci zákonné povinnosti).

Každé zpracování poté musí být evidováno na základě alespoň jednoho titulu²³ zpracování osobních údajů. Jakkoli se titul a účel v rámci zpracování často oddělují (jde totiž o dva odlišné koncepty), pro identifikaci titulu je vhodné vést účel v patrnosti. Stanovený účel totiž může pomoci při ověření, zdali je zpracování záznamů událostí přiměřené a nezbytné, tedy zda by nešlo dosáhnout stanoveného účelu s menším rozsahem zpracovávaných osobních údajů. Jde o jedny ze základních zásad obsažených v článku 5 GDPR.

Nad rámec shora uvedených titulů teoreticky připadá v úvahu ještě souhlas se zpracováním²⁴. V případě souhlasu je však prakticky problematické, že musí být oddělitelný. Jinými slovy v případě, že je využitý jako titul pro zpracování a subjekt údajů jej odmítne dát, musí mu být služba, ke které se váže zpracování, poskytnuta na základě jiného právního titulu pro zpracování osobních údajů. Zároveň souhlas nelze, v důsledku nerovného vztahu, vyžadovat po zaměstnancích organizace. Souhlas je také kdykoli odvolatelný. V praxi je tak jeho využití v kontextu SIEM natolik problematické, až je možné uzavřít konstatováním jeho nevhodnosti.

V souvislosti se zpracováním osobních údajů je pak také důležité zmínit zvláštní kategorii osobních údajů. Osobní údaje zvláštní kategorie jsou údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě

²³ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 321 – 344.

²⁴ URŠIČ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, s. 70 – 71.

nebo sexuální orientaci fyzické osoby.²⁵ V některých případech hrozí, že tyto osobní údaje budou součástí zpracování záznamů událostí.

V případě zpracovávání osobních údajů zvláštní kategorie²⁶ je potřeba jednak naplnovat právní titul, ale také je nutné splňovat některý z dodatečných právních titulů stanovených článkem 9 nařízení GDPR.²⁷ Pokud tyto podmínky nejsou splněny, je zpracování osobních údajů zvláštní kategorie zakázáno.

Je třeba mít na paměti základní principy GDPR, tedy zásady přiměřenosti, minimalizace zásahu, zákonnosti a vymezení účelů zpracování. Proto má ke zpracování docházet jen tam, kde je to účelné a na tak dlouho jak je to potřebné k naplnění stanoveného účelu. Nelze tak stanovit jednotnou dobu, ale je potřeba vždy posuzovat zpracování s ohledem na jeho účel.

3.4 ZEK

ZEK pracuje s provozními a lokalizačními údaji, vůči kterým mají provozovatelé veřejné komunikační sítě nebo poskytovatelé veřejné dostupné služby elektronických komunikací zákonné povinnosti uchovávat je po dobu stanovenou tímto zákonem. V souvislosti s uchováváním událostí se s provozními a lokalizačními údaji pojí dva typy povinností. První z nich jsou obecné, které vyplývají z § 90 ZEK a § 91 ZEK.²⁸ Obecné povinnosti stanovují, že je možné provozní údaje a lokalizační údaje uchovávat po dobu provozu. Poté je potřeba tyto údaje odstranit anebo anonymizovat, pokud nedojde k využití výjimek uvedených v § 90 ZEK.²⁹ V případě zpracovávání lokalizačních údajů, které nejsou provozními údaji, mohou být údaje vztahující se k uživateli nebo účastníku zpracovávány pouze v roz-

²⁵ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 365 – 385.

²⁶ Například údaje v záznamech zdravotního vyšetření nebo informace o návštěvě webových stránek pro pacienty s atypickou vážnou nemocí.

²⁷ Tím může být například zpracování, které je nutné pro splnění povinností a uplatnění práv v pracovním a sociálním právu, pokud to dovoluje právo Unie nebo státu a jsou zajištěny potřebné záruky.

²⁸ CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, s. 390 – 396.

sahu a trvání nezbytném pro poskytování služeb s přidanou hodnotou, a to za předpokladu odvolatelného souhlasu.³⁰ Speciální kategorie je spojena s povinnostmi uchovávat záznamy událostí po dobu 6 měsíců dle § 97 ZEK.³¹ Tato speciální kategorie se váže na ty typy záznamů událostí, které jsou vymezeny ve vyhlášce č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. U těchto záznamů je povinnost zaznamenávat především:

- Datum a čas komunikace,
- komunikující stanice,
- dobu spojení,
- množství přenesených dat,
- identifikátory účastníků.

Pro účely splnění této povinnosti se údaje o času musejí uchovávat v místním čase. Pakliže daný místní čas neodpovídá času v České republice, musí být údaje o čase uváděny s označením časového pásma. Provozní a lokalizační údaje požadované vyhláškou (výše uvedená druhá kategorie) zároveň musí být dle § 4 této vyhlášky po uplynutí šestiměsíční doby zlikvidovány.

Poskytovatel veřejně dostupné služby elektronických komunikací nebo osoba zajišťující veřejnou komunikační síť musí zároveň zajistit bezpečnost a integritu veřejných komunikačních sítí a služeb elektronických komunikací dle § 98 ZEK.³² I při plnění této povinnosti může dojít k potřebě zpra-

²⁹ Výjimky pro provozní údaje jsou obsaženy v § 90 odst. 3 – 6 ZEK: Odst. 3 – Povinnost uchování provozních údajů poskytnutých účastníkovi či uživateli dokud nebude rozhodnuto o sporu dle § 129 odst. 3 ZEK nebo uplynutí doby pro právní napadení vyúčtování ceny či uplynutí doby možného vymáhání úhrady; Odst. 4 – Možnost zpracovávat provozní údaje nezbytné pro vyúčtování ceny do konce doby, během níž může být úhrada vymáhána; Odst. 5 – Možnost předávání dat mezi provozovateli a poskytovateli pro účely vzájemného vyúčtování nebo pro účely identifikace zneužívání sítě a služeb elektronických komunikací; Odst. 6 – Podnikatel poskytující veřejně dostupnou službu elektronických komunikací může, za předpokladu odvolatelného souhlasu, zpracovávat osobní údaje pro poskytování služeb s přidanou hodnotou či pro marketing, a to v nezbytném rozsahu a po nezbytně nutnou dobu.

³⁰ Pokud uživatel či účastník souhlas neučiní, musí se údaje anonymizovat.

³¹ CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, s. 406 - 413.

³² *Ibid.*, s. 423 – 432.

covávat záznamy událostí. V tomto ohledu není právním předpisem stanovena doba uchování záznamu událostí.

3.5 SANKCE ZA NEDODRŽENÍ PRÁVNÍCH POVINNOSTÍ

V důsledku nesprávných parametrů zpracování mohou organizaci uniknout citlivá data, případně může dojít k jejich smazání nebo neplánované změně. V návaznosti na nedostatečné zabezpečení totiž může dojít k reputační škodě nebo snížení provozuschopnosti. Navíc však – což je u organizací s nízkým bezpečnostním povědomím hlavním motivačním faktorem – také může dojít k udělení sankce ze strany dozorujícího správního orgánu. Ilustrativně vybrané příklady sankcí jsou uvedeny v Tabulce 2.

| Právní předpis | Maximální sankce | Cílové subjekty | Příklad porušení |
|---|----------------------------|---|---|
| ZKB14 § 25 odst. 14 písm. a) | 5 mil. Kč | Správce informačního nebo komunikačního systému kritické informační infrastruktury, Správce významného informačního systému | Nezavedení nebo neprovedení bezpečnostních opatření (řízení přístupů), nenahlášení incidentu (např. únik údajů) |
| ZoKB § 59 odst. 1 a odst. 4 písm. a) | 250 mil. Kč / 2 % obrátu | Poskytovatel regulované služby v režimu vyšších povinností | Nezavedení nebo neprovedení bezpečnostních opatření (řízení přístupů), nenahlášení incidentu (např. únik údajů) |
| ZoKB § 59 odst. 2 a odst. 4 | 175 mil. Kč / 1,4 % obrátu | Poskytovatel regulované služby v režimu nižších po- | Nezavedení nebo neprovedení bezpečnostních opatření (řízení |

| | | | |
|--|--------------------------|---|--|
| písm. b) | | vinností | přístupů), nenahlášení incidentu (např. únik údajů) |
| ZEK § 118 odst. 14 písm. j) a odst. 26 písm. b) | 15 mil. Kč / 5 % obratu | Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací | Ohrožení důvěrnosti zpráv a s nimi spojených provozních a lokalizačních údajů (§ 89 odst. 1 nebo § 91 odst. 2, 3 nebo 4) |
| ZEK § 118 odst. 14 písm. c) a odst. 26 písm. c) | 50 mil. Kč / 10 % obratu | Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací | Neuchování či nepředání provozních a lokalizačních údajů, nelikvidování po uplynutí doby, ... (§ 97 odst. 3) |
| ZEK § 118 odst. 16 a odst. 26 písm. b) | 15 mil. Kč / 5 % obratu | Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací | Nesplnění některé z povinností při zabezpečení ochrany údajů (§ 88a odst. 1 nebo 2) |
| GDPR článek 83 odst. 4 písm. a) | 10 mil. EUR / 2 % obratu | Všechny organizace zpracovávající osobní údaje | Nezavedení pseudonymizace nebo jiných opatření (čl. 32) |
| GDPR článek 83 odst. 5 písm. a) | 20 mil. EUR / 4 % obratu | Všechny organizace zpracovávající osobní údaje | Porušení zásad zpracování osobních údajů (čl. 5) |

Tabulka 2: Příklady sankcí za porušení platné legislativy

4. PROCESY SMĚŘUJÍCÍ K NAPLNĚNÍ PRÁVNÍCH POŽADAVKŮ

4.1 NASTAVENÍ DOBY PRO ZPRACOVÁNÍ ZÁZNAMŮ UDÁLOSTÍ

V praxi je možné, že se na konkrétní záznamy událostí bude vztahovat více právních předpisů³³, kdy každý z těchto právních předpisů bude vyžadovat jinou dobu pro jejich uchování. Tento problém si lze představit při aplikaci pravidel plynoucích ze ZEK a ZoKB. Údaje uchovávané podle obou předpisů se budou často obsahově překrývat. ZEK stanoví na jednu stranu povinnost obecné údaje ihned smazat nebo anonymizovat, na stranu druhou uchovávat speciální kategorii údajů po dobu 6 měsíců, zatímco ZoKB, respektive VVR, povinnost uchovávat záznamy událostí alespoň po dobu 18 měsíců. Na první pohled tak dochází ke střetu dvou právních předpisů.

V úvahu připadá aplikace derogačních pravidel (pravidlo právní síly, pravidlo času a pravidlo speciality). Pakliže by k aplikaci derogačních pravidel došlo, pravděpodobně by na základě použití pravidla právní síly byl uplatněn ZEK před pravidly plynoucími z prováděcích předpisů ZoKB. Druhou teoretickou možností je derogační pravidla neuplatnit vůbec a ponechat souběžné působení obou právních předpisů, a to na základě rozdílného účelu právních norem. Účelem ustanovení v ZEK je, v případě § 91, zajištění přenosu zprávy sítí elektronických komunikací (a případně účtování služby) nebo, v případě § 97 ZEK, vyšetřování trestné činnosti a zpravodajská činnost. ZoKB oproti tomu cílí na zajištění kybernetické bezpečnosti pro zajištění řádného poskytování regulovaných služeb. Současné uplatnění pravidel obou předpisů není vyloučeno ani povahou zpracovávaných dat³⁴ a v případě využívání těchto dat v souladu s titulem, na základě kterého jsou zpracovávána, ani nedojde k negativnímu dopadu na subjekt údajů.

Důsledkem uplatnění derogačních pravidel by bylo smazání všech údajů vyžadovaných ZEK v případě, kdy vyprší právní titul, který ZEK poskytuje. V takovém případě by byly zbývající uchovávané údaje dle ZoKB s vysokou

³³ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 193-195.

³⁴ Zejména z toho důvodu, že zpracovávaná data mohou být fyzicky či logicky oddělena.

pravděpodobností nevyužitelné. Oproti tomu uplatnění druhého přístupu zachovává smysl a účel všech předpisů a navíc jej lze vyřešit také po stránce technologické implementace. Z tohoto důvodu byla v textu rozpracována právě tato druhá varianta včetně popisu možné implementace v organizaci. V tomto případě k oprávnění uchovávat záznam událostí postačí, aby jeho uchování svědčila alespoň jedna lhůta daná právním předpisem anebo stanovena organizací v souladu s tímto právním předpisem. Zároveň není nezbytné (a ani účelné, např. s přihlédnutím k nákladům na uchovávání), aby byly uchovávané záznamy událostí duplikovány na více místech. Postačí jejich zaznamenání na jednom místě a evidence jednotlivých oprávnění zpracovávat záznam událostí bude vedena jako příznak záznamu událostí. Po uplynutí rozhodné doby vztahující se k právním předpisům či interním potřebám bude nezbytné, aby byl příznak ze záznamu událostí odstraněn manuálně nebo na základě automatické expirace (mohou však zůstat příznaky plynoucí z jiného právního předpisu). Pakliže je záznam naprosto bez příznaků, musí se smazat anebo musí být anonymizován.³⁵ Do úvahy připadá také zavedení určité *grace period*, tedy přechodného období, během kterého se administrátor musí rozhodnout, jak dál se záznamem událostí naloží.

Většina záznamů událostí obsahuje osobní údaje. Vzhledem k tomu, že nařízení GDPR samo o sobě nestanovuje lhůtu pro uchování záznamu událostí, ale buďto odkazuje na plnění dalších zákonných povinností (plnění zákonných povinností) anebo vyžaduje posouzení pro daný případ zpracování (oprávněný zájem), může být na všechna zpracování záznamů událostí nahlíženo jako by obsahovala osobní údaje. Tento přístup je účelný z hlediska alokace zdrojů (klasifikace může být personálně, časově či finančně náročná) a také z určité procesní opatrnosti. Pokud jsou záznamy událostí zpracovávány za účelem plnění zákonných povinností, lze automaticky nastavit uchování těchto záznamů v souladu s požadavky relevantního právního předpisu.

³⁵ Jiným řešením může být uchovávání různých datasetů pro různé potřeby. V těchto datasetech by byly obsaženy pouze údaje vyžadované např. ZEK, které by byly po nastání rozhodné skutečnosti smazány, zatímco dataset ZoKB by byl naprosto nedotčen.

V souvislosti s osobními údaji je nezbytné dbát na to, aby byly plněny povinnosti správce vůči subjektům údajů. Správce má především povinnost subjekty údajů vhodným způsobem informovat³⁶ o tom, že jsou jejich osobní údaje zpracovávány. Tato informační povinnost musí být naplněna přiměřeně povaze a okolnostem daného zpracování – to znamená, že subjekty musí obdržet jasné, srozumitelné a úplné informace o účelu zpracování, právním základu, době uchování údajů, případných příjemcích a také o svých právech dle kapitoly III nařízení GDPR.³⁷

Součástí odpovědného zpracování je rovněž povinnost zabezpečit osobní údaje přiměřeným způsobem v souladu s článkem 32 nařízení GDPR.³⁸ To zahrnuje přijetí technických a organizačních opatření, která zohledňují aktuální stav techniky, povahu, rozsah, kontext účely zpracování, jakož i rizika pro práva a svobody fyzických osob. V tomto ohledu je často zmiňována anonymizace, která představuje způsob zpracování osobních údajů, při kterém dojde k takové úpravě dat, jež znemožní zpětnou identifikaci fyzických osob, kterých se původně týkala.³⁹ Po provedení anonymizace přestávají být tyto údaje považovány za osobní a nevztahuje se na ně nařízení GDPR.

Navzdory častému přesvědčení, že odstraněním přímých identifikátorů lze data učinit anonymními, judikatura Soudního dvora EU ukazuje, že skutečná anonymizace je v praxi velmi obtížně dosažitelná. Soudní dvůr EU zdůraznil,⁴⁰ že pseudonymizace sama o sobě neznamená anonymizaci – pokud existují prostředky, o nichž lze rozumně předpokládat, že by mohly vést k opětovné identifikaci osob, jak je tomu při propojení s jinými databázemi či při technologickém rozvoji, údaje zůstávají osobními a nadále se

³⁶ Toto informování může být vyřešeno například oznámením na webových stránkách organizace.

³⁷ URŠIČ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, s. 69-70.

³⁸ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 630 – 639.

³⁹ Viz rec. 26 nařízení GDPR.

⁴⁰ Rozsudek SDEU (prvního senátu) ze dne 4. 11. 2025 ve věci C-413/23 P, EDPS v SRB (Notion de données à caractère personnel), body 71–75, 80–86.

na ně vztahuje GDPR. Pouhé technické oddělení doplňujících informací (např. klíčů k přiřazení) proto nestačí. Tento výklad je v souladu i s pokyny EDPB 01/2025. Z tohoto důvodu je namístě zacházet i s údaji považovanými za anonymizované tak, jako by šlo o vysoce pseudonymizované osobní údaje, které stále podléhají pravidlům GDPR. Pro tyto účely je vhodné v organizaci postupovat jednotně a v koordinaci s pověřencem pro ochranu osobních údajů.

Zároveň je potřeba zkoumat, zdali určité zpracování záznamů událostí nepředstavuje při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, vysoké riziko pro práva a svobody fyzických osob. Pokud je vysoké riziko identifikováno, je potřeba, aby organizace zpracovala *Data Protection Impact Assessment* (dále také jen “DPIA”) podle článků 35 a 36 nařízení GDPR.⁴¹ DPIA je potřeba provést v případech:

1. systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
2. rozsáhlého zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nařízení GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 nařízení GDPR; nebo
3. rozsáhlé systematické monitorování veřejně přístupných prostorů.

V případě podezření na povinnost zpracování DPIA je namístě zavést pravidelnou kontrolu změn, v důsledku kterých by mohlo být nakonec nutné DPIA provést. Zároveň by osoby (oddělení, organizační složky) měly spolupracovat s pověřencem pro ochranu osobních údajů organizace, případně s jinou osobou odpovědnou za zajištění souladu s nařízením GDPR.

⁴¹ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 665 – 697.

Také je důležité mít stanovenou obecnou dobu pro uchování záznamů událostí i pro záznamy událostí, u kterých právní předpisy nestanoví konkrétní dobu pro zpracování anebo u kterých doba již uplynula a je účelné a možné je uchovávat dále. Stanovení obecné doby mitiguje právní riziko spojené s nesprávnou klasifikací (například když údaje nebudou označeny za osobní, ač se o osobní údaje jedná) a zároveň bezpečnostní riziko spojené s nepřiměřeným uchováváním záznamů.⁴²

4.2 VYBRANÉ OTÁZKY K ZABEZPEČENÍ ZÁZNAMŮ UDÁLOSTÍ

V souvislosti s uchováváním záznamů je potřeba řídit přístup ke zpracování a zabezpečit zpracování záznamů událostí. Požadavky směřující k zajištění kybernetické bezpečnosti lze nalézt implicitně nebo explicitně v § 88–91, 97, 98 ZEK, dále ZoKB v rámci VVR a VNR a také v článku 32 nařízení GDPR.

Nehledě na legislativu, která se na dané zpracování a uchovávání záznamů událostí aplikuje, je vhodné vycházet z pravidel uvedených ve VVR – a to z toho důvodu, že dává nejdetailejší popis pro zavedení opatření s ohledem na zabezpečení dostupnosti, důvěrnosti a integrity zpracovávaných dat a informací.⁴³ Základním kamenem pro řešení bezpečnosti je ve VVR řízení rizik, od kterého by se mělo odvíjet zavádění dalších bezpečnostních opatření v oblastech ve vyhlášce uvedených.⁴⁴ Tato bezpečnostní opatření ve většině případů představují obecné požadavky, jejichž cílem je nechat k jejich realizaci co největší prostor pro přizpůsobení individuálním podmínkám organizace.⁴⁵

Detailnější rozpis bezpečnostních opatření přesahuje rámec tohoto článku. Proto je nezbytné projít jednotlivé právní předpisy, případně se po-

⁴² Může se jednat například o zastaralé šifrování uchovávaných údajů, a jejich stále narůstající objem, který musí být spravován.

⁴³ JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Šesté, doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025, s. 109.

⁴⁴ Pro naplnění opatření je vhodné vytvořit a srozumitelně komunikovat interní metodiku s jasně stanovenými pravidly, odpovědnostmi, nástroji a kontrolními postupy.

⁴⁵ Např. § 14 VVR řízení přístupu na základě rolí. Jak je vidět, zákonodárce nechal konkrétní realizaci (typy rolí, jejich oprávnění apod.) na organizaci.

radit s odpovědnými osobami v rámci organizace. V souvislosti se zpracováváním záznamů událostí byly v rámci VVR identifikovány jako relevantní především ustanovení § 7 (řízení aktiv), § 13 (řízení přístupů), (§ 15 řízení kontinuity), § 16 (audit), § 19 (požadavky na autentizaci a autorizaci), § 22 (záznamy událostí), § 25 (požadavky na kryptografii), § 26 (testování obnovy) a příloha č. 2 (likvidace dat).⁴⁶

Součástí zabezpečení zpracování záznamů událostí je také hodnocení rizik. Obecně se doporučuje před implementací zbývajících opatření provést hodnocení rizik a realizovat další opatření v souvislosti s ošetřováním jednotlivých rizik, viz § 8 VVR a článek 32 nařízení GDPR. Vyjma toho, že je tento přístup přímo vyžadován ZoKB, umožňuje zároveň efektivnější implementaci opatření i alokaci dostupných zdrojů.

Pro konkretizaci lze zároveň využít různé bezpečnostní standardy např. National Institute of Standards and Technology. *NIST Special Publication 800-92: Guide to Computer Security Log Management*,⁴⁷ který uvádí konkrétní povinnosti spojené se zabezpečením záznamu událostí.

4.3 KONTROLA SOULADU S PRÁVNÍMI POŽADAVKY

Obecně platí, že na počátku je oprávnění ke zpracování záznamů událostí a obsažených osobních údajů (užitečnost jejich uchování) nejsilnější a s postupem doby se tato vlastnost oslabuje a začíná převažovat potřeba jejich odstranění či anonymizace.⁴⁸ Pro případ pochybení nebo změny okolností je vhodné mít nastavený proces kontroly nastavených pravidel pro zpracování záznamů událostí (automatizovanou/manuální). Kontrola nemusí probíhat na úrovni jednotlivých záznamů událostí, ale na úrovni typových zpracování. Pokud dochází ke zpracování záznamů událostí – např. přihlášení informačního systému – může kontrola probíhat na úrovni

⁴⁶ POLČÁK, Radim; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Právo informačních technologií*. 2. vydání. Praha: Wolters Kluwer, 2024, s. 825-829.

⁴⁷ KENT, Karen a SOUPPAYA, Murugiah. NIST SP 800-92. Guide to Computer Security Log Management. In: COMPUTER SECURITY RESOURCE CENTER/NIST [online]. 2006. [cit. 20. 9. 2025]. Dostupné z: <https://csrc.nist.gov/pubs/sp/800/92/final>

⁴⁸ Podobný argument v jiném kontextu přináší i SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology*, 2016, roč. 24, č. 1, s. 72-98.

ověření aktuálnosti nastavených pravidel pro daný typ zpracování, nikoli pro každý zvlášť. Záleží ovšem na rizikovosti daného zpracování záznamů událostí a kapacitách organizace.

Kontrola by měla zahrnovat minimálně následující položky:

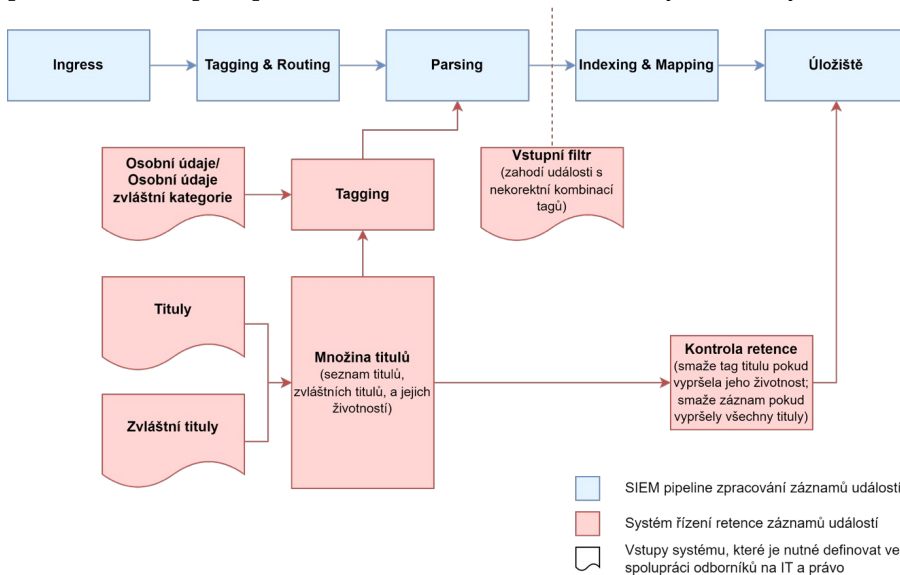
- Zda je splněn alespoň jeden z právních titulů a dodržené podmínky zpracování
- Zda jsou záznamy událostí stále dostupné a pokud hrozí riziko nečitelnosti převést události na jiná média nebo do jiných formátů
- Zda jsou zvolená pravidla zabezpečení skutečně dodržována
- Zda je obsah záznamů událostí správný a korektní

5. TECHNICKÁ IMPLEMENTACE/AUTOMATIZACE IDENTIFIKOVANÝCH POŽADAVKŮ

Tato kapitola je věnována způsobu, kterým je možné implementovat opatření na aktuální SIEM již nasazené v organizacích tak, aby byly v souladu s diskutovanou legislativou. Řízení přístupů je technicky snadno realizovatelné; aktuální SIEM nabízí široké možnosti nastavení zabezpečení přístupů až na úroveň jednotlivých uživatelů a záznamů událostí. Korektní nastavení přístupů tedy závisí více na procesech organizace a jejich dodržování než technické implementaci. Řízení retence záznamů událostí je z pohledu implementace zajímavější problém, který bude podrobněji adresován. Žádný nám známý SIEM toto řízení nativně nepodporuje, lze jej ale implementovat externě běžícím systémem při využití existujících funkcí API SIEM.

Princip navrhovaného systému pro řízení retence záznamů událostí v SIEM vychází z předpokladu, že pro zpracování každého záznamu události je třeba jeden nebo více konkrétních právních titulů, jak je určuje např. nařízení GDPR. Tyto právní tituly je nutné určit již při vstupu záznamu události do SIEM a uchovávat je u něj po celou dobu zpracování. Zároveň je nutné počítat s tím, že právní tituly pro zpracování mají typicky omezenou životnost, danou některým z relevantních předpisů (např. ZoKB, ZEK). Po celou dobu přítomnosti záznamu události v SIEM je tedy nutné sledovat,

kteřé právní tituly pro zpracování již pominuly a v případě expirace všech právních titulů pro zpracování daného záznamu tento vyřadit ze systému.



Obrázek 1: Schéma pipeline pro zpracování záznamů událostí se zapojením navrhaného systému pro řízení retence

Před pojednáním o návrhu implementace systému pro řízení retence je třeba stručně popsat co se rozumí pod termínem pipeline pro zpracování záznamů událostí. Obecně řečeno, jde o řetězec modulů nebo funkcí v rámci SIEM, které postupně mění typicky nestrukturovaný záznam události na vstup na strukturovaný a otypovaný záznam, použitelný pro analytické funkce uživatelské vrstvy SIEM. Příklad takové pipeline je zobrazen na schématu na Obrázku 1 (modrá barva). Prvním modulem, do něhož záznam události v SIEM zpravidla vchází, je *Ingress*. Zde je dešifrován a je ověřena jeho autenticita. Druhým modulem je *Tagging & Routing*. Zde jsou záznamu události přiřazeny interní značky (tagy), pomocí nichž je směrován do příslušných větví pipeline. V jedné pipeline tak může být zpracováváno více druhů záznamů událostí, které vyžadují rozdílné metody zpracování. Třetím modulem je *Parsing*. Zde dochází k extrakci informací ze záznamu události. Modul transformuje záznamy událostí, mnohdy ve formě prostého

textu, do podoby strukturovaných dat, která je poté možné automatizovaně zpracovávat. Čtvrtým modulem je *Indexing & Mapping*, kde je pro každou položku nyní strukturovaného záznamu události určen nejvhodnější typ, např. IP adresa, textový řetězec, nebo časová známka, a záznamy událostí jsou optimalizovány pro vyhledávání. Teprve poté je záznam událostí uložen na centrálním SIEM úložišti a mohou k němu přistupovat uživatelé systému.

Návrh implementace algoritmu pro řízení retence událostí je znázorněn na Obrázku 1 (červená barva). Pro přehlednost je potřeba prvně uvést, jak systém ovlivní průchod záznamu události SIEM pipeline a poté, jak lze jednotlivé moduly systému implementovat. Konec kapitoly je věnován výhodám i nevýhodám systému, a otevřeným otázkám, které je nutné před nasazením systému vyřešit, zejména s ohledem na pokročilejší automatizaci.

Zpracování záznamů událostí v SIEM pipeline ovlivní systém poprvé v modulu *Parsing*, do které zasahuje modulem *Tagging*. Modul je posunutý nad úroveň *Tagging & Routing* modulu v pipeline z toho důvodu, že až v *Parsing* modulu dochází k extrakci všech relevantních informací ze záznamu událostí. Typicky teprve zde je možné nejspolehlivěji odlišit osobní údaje zvláštní kategorie a určit příslušné právní tituly zpracování. Na základě výše uvedených informací lze očekávat, že naprostá většina zpracovávaných záznamů bude spadat do údajů regulovaných nařízení GDPR. *Tagging* modul tedy nejprve označí každý záznam události procházející pipeline buď jako osobní údaj, nebo osobní údaje zvláštní kategorie. Poté modul přiřadí záznamu události jeden nebo více tagů odpovídajících výběru z množiny všech možných právních titulů pro zpracování. Z modulu odchází záznam události obohacen o všechny informace, které jsou nezbytné k vyhodnocení oprávněnosti zpracování a k určení délky retence.

Záznam události následně musí projít modulem *Vstupní filtr*. Tento filtr zahazuje záznamy událostí bez tagů, nebo s nevyhovující kombinací tagů, aby nedošlo ke zpracování záznamů událostí, pro které nebyl naplněn odpovídající titul. Např. filtr zahodí všechny záznamy, u nichž není žádný tag titulu, nebo záznamy obsahující osobní údaje zvláštní kategorie, kterým

není přidělen zvláštní právní titul. Filtr zajišťuje, že záznamy událostí, u nichž by hrozilo nedostatečně odůvodněné zpracování, jsou zahozeny ihned, jak je nedostatečnost odhalena.

V poslední fázi pipeline zpracování záznamů událostí jsou záznamy událostí uloženy na SIEM úložiště. Na tomto úložišti jsou záznamy spravovány modulem *Kontrola retence*. *Kontrola retence* periodicky, například jednou denně, prochází všechny záznamy událostí na úložišti. Řídí se následující logikou:

1. Pokud se u záznamu událostí nachází tag právního titulu, jehož životnost vypršela, smaž daný tag.
2. Pokud záznam událostí obsahuje osobní údaje zvláštní kategorie a zároveň nemá tag zvláštního právního titulu, smaž daný záznam.
3. Pokud záznam událostí nemá žádný tag titulu, smaž daný záznam.

Na úložišti by se tak neměly nacházet neodůvodněně zpracovávané záznamy událostí déle, než je nastavená perioda běhu modulu.

Moduly námi navrhovaného systému pro řízení retence lze implementovat částečně s využitím existujících funkcí SIEM, částečně jako vlastní kód. Modul *Tagging* je postavený na funkci SIEM, která umožňuje přidat každé události libovolné tagy. Tato funkce již při zpracovávání záznamů událostí obvykle bývá využita, a to pro směrování záznamů událostí do různých větví pipeline. Kategorie osobních údajů a tituly pro zpracování lze tedy uvádět přímo do konfigurace SIEM. *Vstupní filtr* je rovněž implementovatelný na úrovni SIEM, jako další modul včleněný do pipeline pro zpracování záznamů událostí. Poslední modul systému, *Kontrola retence*, přesahuje obvyklé možnosti SIEM a nejspíš bude muset být provozován externě. V principu jde ale o jednoduchý algoritmus, implementovatelný periodicky spouštěným skriptem, který volá příslušné SIEM funkce (přečti záznam, smaž položku, smaž záznam) přes jeho API. Pro modul postačí např. kombinace Python skriptu spravovaného v plánovači Temporal.⁴⁹

Kromě zajištění souladu retence dat v SIEM s legislativou platnou v České republice, má navrhovaný model následující výhody:

⁴⁹ Temporal. Webové sídlo. Dostupné z: <https://temporal.io/> [cit. 20. 9. 2025].

1. Škálovatelnost – všechny vstupy (kategorie osobních údajů, tituly, pravidla vstupního filtru) je možné jednoduše rozšiřovat a reagovat tak na změny v legislativě.
2. Granularita – retenci je možné nastavovat a kontrolovat až na úroveň jednotlivých záznamů událostí. Aktuálně je běžná různá retence pouze na úrovni kategorií záznamů událostí.
3. Snadný auditing – u každého záznamu události v SIEM je jasně stanoveno, z jakých titulů je zpracováván.

Na druhou stranu, zásadní nevýhodou systému je závislost na statické manuální konfiguraci, a to zejména u identifikace osobních údajů zvláštní kategorie. V současnosti je možné použít nastavení pipeline, kde například záznamy událostí z obecných webových serverů instituce budou staticky kategorizovány jako osobní údaje, zatímco záznamy z podмноžiny webových serverů poskytujících zdravotní služby, budou preventivně kategorizovány jako osobní údaje zvláštní kategorie. Takové statické nastavení je těžkopádné a náchylné k omylu, ale bohužel aktuálně neexistují nástroje, které by kategorizaci alespoň částečně automatizovaly.

S výše zmíněnou závislostí na statické konfiguraci závisí i otevřené otázky, které je třeba před nasazením systému vyřešit. Zejména jak lépe automatizovat:

1. Plnění množiny titulů – aktuálně řešení spoléhá na periodické kontroly právních předpisů, identifikaci účelů pro zpracování, a manuální přepis do tagů.
2. Stanovení pravidel pro vstupní filtr – primárním pramenem jsou pravidla obsažena v nařízení GDPR pro kategorie osobních dat a tituly pro zpracování.
3. Rozlišení osobních údajů zvláštní kategorie – kategorii lze nyní pouze odhadnout na základě typu zařízení a služeb, ze kterých jsou záznamy sbírané, a analýzy informačního obsahu vzorku záznamů událostí.

U otevřených otázek je plná automatizace převodu právních předpisů do praxe jen stěží uskutečnitelná, protože prostředí, na něž se tyto předpisy vztahují, je příliš proměnlivé. V tom případě je třeba alespoň definovat pro-

cesy pro provádění a kontrolu převodu daných pravidel ve spolupráci odborníků na právo a informační technologie.

6. ZÁVĚR

Tento článek představil problematiku uchovávání a správy bezpečnostních informací a událostí v organizaci z pohledu požadavků kladených legislativou a navrhuje právní i technické řešení souběžné aplikace více legislativních požadavků na konkrétní údaje. V rámci toho došlo k odpovědi na dvě stanovené výzkumné otázky:

Jaké jsou požadavky právních předpisů na stanovení doby uchování a zabezpečení záznamů událostí zpracovávaných logovacím nástrojem? Nakládání se zpracovávanými daty je v různých předpisech řešeno různě, avšak na základě povahy ukládaných údajů a odlišných účelů legislativy mohou být tyto požadavky aplikovány souběžně. Některé povinnosti jsou vymezeny konkrétně (ZEK), minimální dobou (ZoKB) nebo jsou ponechány na posouzení organizace (oprávněný zájem dle nařízení GDPR). Nastavení pravidel přístupu k takovýmto datům je primárně v režii dotčené organizace.

Jaké jsou technické možnosti implementace právních požadavků na uchovávání údajů? Technické provedení navrženého právního řešení je založeno na tagování (štítkování) jednotlivých záznamů podle účelu jejich zpracování v kombinaci s ověřováním aktuality jednotlivých tagů a nastavením pravidel pro případ, že tagy již aktuální nebudou, neboť účely zpracování vyprší. Navržené řešení se neobejde bez lidského zásahu, co se týče klasifikace zpracovávaných údajů, identifikace titulů pro zpracování a nastavení doby uchování. Po uskutečnění těchto kroků však dokáže fungovat automatizovaně a zároveň nabízí praktické vlastnosti v podobě škálovatelnosti, uzpůsobení granularity a jednoduché auditovatelnosti.

7. SEZNAM POUŽITÝCH ZDROJŮ

- [1] ALI, Sijjad; WANG, Jia a LEUNG, Victor Chung Ming. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms- A comprehensive review. *Information Fusion*. [online]. 2025, roč. 118, s. 1-45. [cit. 20. 9. 2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1566253524007000>
- [2] BHATT, Sandeep; MANADHATA, Pratyusa K. a ZOMLOT, Loai. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*. [online]. 2014, roč. 12, č. 5, s. 35-41. [cit. 20. 9. 2025]. Dostupné z: <https://ieeexplore.ieee.org/document/6924640>
- [3] CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, 661 s. ISBN 978-80-286-0151-5.
- [4] GONZÁLEZ-GRANADILLO, Gustavo, GONZÁLEZ-ZARZOSA, Susana and DIAZ Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. [online]. 2021, roč. 21, č. 14, s. 1-38. [cit. 20. 9. 2025]. Dostupné z: <https://www.mdpi.com/1424-8220/21/14/4759>
- [5] JIRÁSEK, Petr; NOVÁK, Ludík a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Šesté, doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025, 396 s. ISBN 978-80-53054-00-3.
- [6] KENT, Karen a SOUPPAYA, Murugiah. NIST SP 800-92 Guide to Computer Security Log Management In: COMPUTER SECURITY RESOURCE CENTER NIST [online]. 2006. [cit. 20. 9. 2025]. Dostupné z: <https://csrc.nist.gov/pubs/sp/800/92/final>
- [7] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, 1393 s. ISBN 978-0-19-882649-1.
- [8] LIU, Che-Wei; HUANG, Peng a LUCAS, Henry C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*. [online]. 2019, roč. 37, č. 3, s. 758 - 787. [cit. 20. 9. 2025]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850178
- [9] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2015, 219 s. ISBN 978-80-7478-817-8.
- [10] MENGES, Florian, Tobias LATZO, Manfred VIELBERTH, Sabine SOBOLA, Henrich C. POHLS, Benjamin TAUBMANN, Johannes KOSTLER, Alexander PUCHTA, Felix FREILING, Hans P. REISER a Günther PERNUL. Towards GDPR-compliant data processing in modern SIEM systems, *Computers & Security*, 2021, sv. 103, 102165.
- [11] NONNEMANN, František; ÈERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025, 258 s. ISBN 978-80-286-0331-1.

- [12] POLČÁK, Radim; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Právo informačních technologií*. 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2024, 955 s. ISBN 978-80-286-0059-4.
- [13] Rozsudek SDEU (prvního senátu) ze dne 4. 11. 2025 ve věci C-413/23 P, Evropský inspektor ochrany údajů v. SRB (Notion de données à caractère personnel), ECLI:EU:C:2025:645.
- [14] SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology*, 2016, roč. 24, č. 1, s. 72-98. ISSN: 0967-0769
- [15] SASHWIN, K; NITHIKA, K S; PRIYADHARSHINI, S; MADUVANT, S P a SARANYA. Analysis, Trends, and Utilization of Security Information and Event Management (SIEM) in Critical Infrastructures. *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)*. [online]. 2024, s. 1980-1984. [cit. 20. 9. 2025]. Dostupné z: <https://ieeexplore.ieee.org/document/10717237>
- [16] *Temporal*. Webové sídlo. Dostupné z: <https://temporal.io/> [cit. 20. 9. 2025].
- [17] URŠIÈ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, 268 s. ISBN 978-0-19-886842-2.
- [18] VELÁSQUEZ, Juan, Miguel, Lopez; MONTERRUBIO, Sergio, Mauricio, Martínez; CRESPO, Luis, Enrique, Sánchez a ROSADO, David, Garcia. Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*. [online]. 2023, roč. 22, s. 691-711. [cit. 20. 9. 2025]. Dostupné z: <https://link.springer.com/article/10.1007/s10207-022-00657-9>

Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).
