Ministerstvo
zdravotnictví

Odpověď Ministerstva zdravotnictví na žádost o informaci dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane,

k Vámi podané žádosti o poskytnutí informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, doručené Ministerstvu zdravotnictví (dále jen „MZd“) dne 5. 8. 2026, evidované pod č. j.: xxx, ve věci níže uvedených dotazů,

„***1. Zadání, schválení a časový průběh auditu/monitoringu***
– kopii konečného schváleného zadání, rozhodnutí, pokynu nebo objednávky, na jejichž základě byl audit/monitoring zahájen;
– sdělení jeho účelu, data zahájení a ukončení a jména a funkce osoby, která jej schválila, včetně označení útvaru odpovědného za převzetí výsledků.
2. Dodavatel, smluvní základ a náklady
– identifikaci externího dodavatele a případných poddodavatelů a kopii smlouvy nebo objednávky, dodatků, předávacího či akceptačního protokolu a faktur vztahujících se k auditu/monitoringu;
– sdělení celkové sjednané, fakturované a uhrazené částky včetně DPH, použitého způsobu výběru dodavatele a identifikátoru uveřejnění smlouvy nebo objednávky v registru smluv, pokud se na daný dokument vztahovala povinnost uveřejnění.
3. Způsob a rozsah monitoringu
– kopii technického nebo metodického popisu monitoringu, název použitého software a přehled kategorií shromažďovaných nebo vyhodnocovaných údajů, zejména zda šlo o údaje o používaných aplikacích, navštívených internetových stránkách, době aktivity, obsahu obrazovky nebo komunikaci;
– sdělení počtu monitorovaných osob a zařízení, dotčených organizačních útvarů, doby sběru dat, zda sběr probíhal i mimo pracovní dobu nebo při práci na dálku a zda byly údaje spojovány s konkrétní osobou, účtem nebo zařízením.
4. Výstupy, analýzy a jejich příjemci
– kopii závěrečné zprávy a dalších konečných analýz, prezentací nebo tabulkových výstupů předaných ministerstvu;
pokud byly vytvářeny individuální výstupy o jednotlivých zaměstnancích, žádám rovněž o tři anonymizované příklady takového výstupu a příslušnou metodickou vysvětlivku;
– sdělení, kterým funkcím nebo organizačním útvarům byly údaje a výstupy zpřístupněny, kdo byl jejich konečným uživatelem a k jakému účelu měly být využívány.
5. Posouzení zákonnosti a ochrana osobních údajů
– kopii existujícího konečného právního posouzení, vyjádření pověřence pro ochranu osobních údajů a posouzení vlivu na ochranu osobních údajů (DPIA), bylo-li provedeno, případně dokumentu, který zaznamenává závěr, že DPIA nebylo nutné;
– kopii existujícího posouzení souladu monitoringu s GDPR a § 316 zákoníku práce, informací poskytnutých zaměstnancům o rozsahu a způsobu kontroly a dokumentu určujícího dobu uchování a způsob výmazu nebo anonymizace získaných údajů.
6. Využití výsledků, námitky zaměstnanců a následná kontrola
– sdělení, zda byly výsledky použity při individuálním prověřování zaměstnanců nebo při pracovněprávních či služebních opatřeních, v kolika případech, a zda na jejich základě byla přijata organizační, personální, technická nebo bezpečnostní opatření; v kladném případě žádám o kopii příslušného souhrnného rozhodnutí nebo akčního plánu;
– kopii případného hromadného podání či námitek zaměstnanců a odpovědi ministerstva a sdělení, zda je postup předmětem interního nebo externího prověřování, včetně označení kontrolního orgánu, aktuálního stavu a kopie již existujícího konečného výstupu.“

Vám sděluji následující:

Ministerstvo zdravotnictví
Palackého náměstí 375/4, 128 00 Praha 2
T: +420 224 971 111, E: podatelna@mzd.gov.cz
IČ: 00024341, ID DS: pv8aaxd, mzd.gov.cz

1. V rámci odpovědi odkazujeme na Dohodu o vypořádání vzájemných závazků zveřejněnou v registru smluv na tomto odkazu: https://smlouvy.gov.cz/smlouva/39026798.
Účelem auditu bylo získání objektivního přehledu o stavu informačního a technologického prostředí ministerstva, identifikace případných provozních a kyberbezpečnostních rizik a ověření využívání pracovních prostředků z hlediska bezpečnosti a souladu s interními pravidly. Monitoring probíhal v období od 7. 4. 2026 do 12. 5. 2026. Původní objednávku, stejně jako akceptační protokol, podepsal ministr zdravotnictví Mgr. et Mgr. Adam Vojtěch, MHA. Útvarem odpovědným za věcnou koordinaci a převzetí výstupů byl Kabinet ministra.

2. V rámci odpovědi odkazujeme na Dohodu o vypořádání vzájemných závazků zveřejněnou v registru smluv na tomto odkazu: https://smlouvy.gov.cz/smlouva/39026798. Tento dokument obsahuje veškerá smluvní ujednání včetně konečné finanční částky (s odkazem na § 6 odst. 1 zákona č. 106/1999 Sb.). K danému plnění nedisponujeme žádnou fakturou.
Dle hodnoty předmětné smlouvy se jednalo o tzv. veřejnou zakázku malého rozsahu, jejíž zadávání není upraveno zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, tedy zákon ponechává formu výběru dodavatele na zadavateli. Ministerstvo zdravotnictví provedlo průzkum předmětného trhu s ohledem na specifické požadavky předmětu poptávaného plnění a na základě jeho výsledku bylo rozhodnuto oslovit přímo konkrétního dodavatele.

3. Použitým softwarovým řešením byla služba RYANT Software Audit, označovaná též RSA. Technické prostředky poskytovatele sestávají zejména z RSA Serveru, aplikace RSA Client a analytického modulu RSA Analysis; RSA Client je popsán jako klientská aplikace běžící jako proces na jednotlivých stanicích v síti objednatele, která sleduje spouštěné procesy a informace o nich odesílá serverové aplikaci.
Shromažďovanými provozními a technickými údaji, se rozumí konkrétně titulek aktivního okna, název uživatelského profilu, název počítače a časové razítko. Dále byl v minutových intervalech zaznamenáván čas od poslední aktivity na počítači (idle), název spuštěné aplikace a hardwarová i softwarová konfigurace počítače. Analýza nezahrnovala sběr obsahu e-mailové komunikace, dokumentů ani zpráv, nebyly pořizovány snímky obrazovky, nebyl zaznamenáván obsah navštívených webových stránek a nebyly zaznamenávány stisky kláves.
Rozsah služby se týkal 502 uživatelů napříč celým ministerstvem, byly tedy dotčeny všechny útvary. K dotazu na dobu sběru dat odkazujeme na první odpověď. Sběr dat v rámci uvedeného intervalu se týkal využití pracovního IT vybavení bez časového a místního omezení.
Sbírané provozní údaje byly technicky přiřazovány k doménovému účtu (loginu) a konkrétnímu názvu stanice v doménové síti Active Directory výhradně za účelem identifikace zařízení v síťovém prostředí. Metodický a technický popis vycházel ze standardních funkčních specifikací řešení RSA zaměřených na pasivní mapování běžících procesů.

4. K datům, vždy jen v nezbytném rozsahu, mají přístup pouze osoby, které je potřebují k výkonu svých pracovních povinností, typicky tedy vrchní ředitelé, ředitelé, oddělení IT, oddělení krizového řízení a bezpečnosti. Data mají být využívána v souladu s cílem auditu, tedy k posílení bezpečnosti informačního a technologického prostřední ministerstva a zabezpečení využití IT vybavení v souladu s interními předpisy a platnou legislativou.
Pokud jde o výstupy týkající se jednotlivých pracovních stanic, tyto výstupy byly generovány ve formě agregovaných časových os a procentuálního rozpadu spuštěných procesů (členěných do kategorií: aktivní práce s aplikací, nečinnost systému/idle, webový provoz a systémové procesy). Metodika jejich vyhodnocení spočívala ve statistickém porovnání provozních časů bez jakéhokoliv hodnocení obsahu zpracovávaných dat.

5. Takové dokumenty ve fyzické podobě neexistují. Předmětný audit IT infrastruktury nezahrnoval sledování obsahu zpráv, profilování ani invazivní metody zakládající vysoké riziko pro práva a svobody zaměstnanců ve smyslu čl. 35 GDPR, a vypracování formálního posouzení vlivu na ochranu osobních údajů (DPIA) proto nebylo zákonnou podmínkou. Zaměstnanci jsou o zákazu užívání techniky k osobním účelům i o možnosti přiměřené kontroly informováni ze zákona (§ 316 odst. 1 zákoníku práce)

i platnou Směrnicí k používání ICT na MZd[cite: 1]. Doba uchování a likvidace provozních dat se řídí obecnými pravidly minimalizace údajů.

6. Cílem analýzy nebylo primárně posuzovat jednotlivce a technická data sama o sobě nemohou sloužit jako hodnocení práce konkrétního zaměstnance. Pokud by jakékoli výstupy analýzy měly být v individuálním případě dále řešeny, musely by být nejprve ověřeny, zasazeny do konkrétního kontextu a projednány s dotčeným zaměstnancem. Zjištěné indikátory samy o sobě neprokazují porušení povinnosti konkrétní osobou. Na základě zjištění jsou diskutována opatření směřující ke snížení identifikovaných rizik, včetně omezení přístupu k vybraným kategoriím internetových služeb a sociálních sítí z pracovních počítačů. Povinný subjekt žádné hromadné podání či námitky zaměstnanců neobdržel.