

# KVALIFIKAČNÍ POSUDEK (VZOR)

Fiktivní příklad. Společnost, zjištění a důkazy jsou smyšlené a slouží výhradně k demonstraci dané metody.

Číslo posudku: MZG-2026-014 (příklad)

Datum: 21.09.2026

Vypracoval: Jan Richter, odborník na kvalifikaci v oblasti IT bezpečnosti (metodika GxP)

Objednatel: MUSTERWERK GROUP (fiktivní) – globální průmyslová skupina, dceřiné společnosti v EU v Německu a ČR, roční obrat 500 mil. EUR a více

Oblast působnosti: EU-IT instance společnosti MUSTERWERK GROUP, 180 zaměstnanců, hostování v Azure EU, 4 kritické aplikace, 11 smluv o zpracování údajů s subdodavateli.

Zdroje požadavků: Nařízení GDPR čl. 28, 32, 33; zákon NIS2UmsuCG § 30, § 33, § 38, § 39; zákon č. 264/2025 Sb. o kybernetické bezpečnosti § 13, § 14, § 16; moduly BSI-Grundschutz APP / CLA / ORP.

Metoda: Kvalifikace v rámci tří stupňů pro každé opatření:

- I – Instalace: Je opatření správně nastaveno (konfigurace, zásady, role)?
- O – Provoz: Probíhá nepřetržitě a lze to prokázat (protokoly, hlášení, opakovaná testování)?
- P – Výkon: Vydrží pod tlakem (test, zatížení, scénář útoku/selhání)?

Třídy důkazů (metoda prokázání je uvedena jako nález):

- SAMOSTATNĚ ZÍSKANÉ: Surové důkazy od zadavatele týkající se verzovaných a kontrolními součty ověřených protokolů o kvalifikaci, samostatně získané (surový výstup skriptu, bez jakéhokoli hodnocení); tyto důkazy byly metodicky prověřeny posudkovatelem.
- ŽIVĚ SLEDOVÁNO: Test výkonnosti byl proveden pod dohledem znalce během společného jednání.
- NEOVERITELNÉ: Důkazy nejsou sledovány, nález, jeho hodnocení negativně a nepřejímá se.

## 1. Celkové hodnocení

| Ukazatel | Hodnota |

|---|---|

| Ověřená opatření | 20 |

| Splněno (I+O+P) | 6 |

| Splněno částečně (I v pořádku, chybí O nebo P) | 9 |

| Neuspělo | 5 |

| Připravenost k předložení důkazu o provedení pro dozor | poskytnuto s omezením |

Hlavní závěr: Organizace má dobrou dokumentaci. Je zdokumentováno 15 z 20 opatření. Pouze 6 z 20 opatření lze v současnosti obhájit před kontrolou na základě důkazu o provedení. Právě tento rozdíl mezi zdokumentovanými a skutečně realizovanými opatřeními je důvodem pro uvalení sankcí v předchozích řízeních (CNIL/France Travail 01/2026: opatření identifikovaná v DPIA, avšak neúčinně realizovaná; výše sankce 5 milionů EUR; ANSPDCP/Renault 03/2026: nedostatečný důkaz o přijetí vhodných opatření a řádné kontrole dodavatelů; UODO/Polsko 2025: identifikované riziko bez realizace protipopatření).

## 2. Příklady nálezů (výňatek, 5 z 20)

### B1 - MFA pro administrativní systémy a vzdálený přístup

- Zdroj: GDPR čl. 32 odst. 1 písm. b; NIS2UmsuCG § 30 (Řízení přístupu)
- I – Instalace: SPRÁVNĚ. Směrnice MFA je k dispozici, služba Azure Conditional Access je nakonfigurována.
- O – Provoz: CHYBNĚ. Prokazatelné zavedení platí pouze pro VPN a e-mail. Administrátorské konzole a systém pro lidské zdroje však využívají starší metody autentizace bez MFA (export protokolů přihlášení za 30 dnů; celkem 1 214 administrátorských přihlášení bez MFA).
- P – Výkon: NEOVĚŘENO. Nebyl proveden test, zda směrnice skutečně blokuje přístup po vyloučení druhého faktoru.
- Hodnocení: Částečně splněno. V dokumentaci je uvedeno, že MFA je implementováno všude, avšak skutečná realizace ukazuje, že to neplatí pro privilegované účty. Jedná se o přesný vzor případů „částečného MFA“, které kritizovaly CNIL a EDPB.
- Důkaz o provedení pro dnešní kontrolu je možný: Ne.

## **B2 - Zálohování a možnost opětovného spuštění**

- Zdroj: Nařízení GDPR čl. 32 odst. 1 písm. c (obnovitelnost); NIS2UmsuCG § 30 (obnova)
- I: SPRÁVNĚ. Imutabilní (neproměnné) zálohy jsou nakonfigurovány a harmonogram je zdokumentován.
- O – Provoz: SPRÁVNĚ. Denní pracovní hlášení jsou k dispozici a archivována.
- P: NEUSPĚLO. Poslední zdokumentovaný test obnovy: před 19 měsíci, u jedné z čtyř aplikací.
- Hodnocení: Částečně vyhovující. Článek 32 vyžaduje schopnost obnovy dat, nikoli samotný úkol zálohování. Neotestované zálohy jsou v postupech hodnoceny jako nedostatečné (příklady porušení ochrany osobních údajů podle EDPB, judikatura UODO: bezpečnost musí fungovat i v případě selhání systému).
- Důkaz lze dnes předložit: Částečně (instalace/provoz), nikoli však pro účely prokázání výkonu.

## **B3 - Řízení subdodavatelů (čl. 28)**

- Zdroj: Nařízení GDPR čl. 28 odst. 1; zákon NIS2UmsuCG § 30 (Řízení dodavatelů)
- I: SPRÁVNĚ. Je přítomno 11 AVV; obsahují kontrolní klauzule.
- O: NEUSPĚLO. Chybí jakýkoli důkaz o provedení alespoň jednoho výkonu auditních práv za poslední 3 roky (čl. 28 odst. 3 písm. h). Hodnocení rizik podle AV se provádí pouze při uzavření smlouvy, bez jakékoli periodicity.
- Otázka: NEUSPĚLO. U 8 z 11 smluv o zpracování nebyly provedeny kontroly týkající se záruk (seznamy subdodavatelů, přístup k logům, testy úniku dat).
- Hodnocení: Neprošlo. Povinnost průběžného testování: dlouholetá spolupráce bez provedení testů nepředstavuje dostatečnou záruku (UODO 2025, EDPB ETL 07/2020 odst. 99).
- Důkaz lze dnes předložit: Ne.

## **B4 - Registrace a povinnosti podle BSI**

- Zdroj: NIS2UmsuCG § 33, § 38, § 39
- I: SPRÁVNĚ. Registrace na portálu BSI byla provedena (důkaz o provedení: potvrzení z portálu).
- O: CHYBNĚ. Proces aktualizace změněných údajů (2 týdny, § 33 odst. 5) neexistuje. Změna rozsahu IP adres z června byla aktualizována po 31 dnech.
- P: OTEVŘENO. Důkaz o absolvování školení pro vedení společnosti je k dispozici, avšak neexistuje žádný kontrolní protokol o provedení (postup hlášení nebyl nikdy vyzkoušen; lhůty 24 hodin, 72 hodin a 1 měsíc nebyly nikdy uplatněny).
- Hodnocení: Částečně vyhovující. Od roku 2028 platí povinnost předložit důkaz o provedení podle § 39; současný stav nevyžaduje bezpříčinnou kontrolu plnění povinností vedoucích

pracovníků (čl. 34 směrnice, § 38).

- Důkaz lze dnes předložit: Pro registraci ano, pro dohled nad řízením ne.

## B5 - Šifrování mobilních zařízení

- Zdroj: Nařízení GDPR čl. 25, odst. 1 písm. a
- I: SPRÁVNĚ. Zásada Intune pro BitLocker, výjimková skupina „Terénní technika“ (9 zařízení).
- O: NEUSPĚLO. Výjimka bez náhrady: žádná technická náhrada, žádná kompenzace, žádný časově omezený seznam výrobků, žádná čtvrtletní kontrola.
- Otázka: – (z důvodu chyb v označení nebyla zodpovězena)
- Hodnocení: Neprošlo. Riziko bylo identifikováno, opatření je uvedeno v dokumentaci, avšak jeho realizace trpí dlouhodobými prodlevami: to je ten faktor, který v řízení zakládá hrubou nedbalost, neboť existuje důkaz o tom, že riziko bylo známo (UODO 2025: „Poznání rizika bez přiměřených nápravných opatření má větší váhu než samotný nedostatek analýzy“).
- Důkaz lze dnes předložit: Ne.

---

## 3. Plán prioritních nápravných opatření (výňatek)

| Priorita | Opatření | Náklady | Cíl důkazu |

|---|---|---|---|

| 1 | MFA na všech privilegovaných systémech, starší metody ověřování vypnuty | 2-3 týdny | O+P: 30denní deník + test uzamčení |

| 1 | Test obnovy všech 4 aplikací, každé čtvrtletí | 1 týden na jeden cyklus | O+P: Zpráva o obnově + schválení |

| 2 | Cyklus auditů AV: 11 AVV, rizikově orientovaný, zahájení prostřednictvím platebního styku | Auditní slot je AVV | Předmět: Auditní zprávy, důkazy o provedení subprocessorů |

| 2 | Oblast technologií: Vyřešení výjimky pro Intune (klient Exchange On-Prem), seznam produktů na vyřazení | 2 týdny | I+O: Export konfigurace, čtvrtletní důkazy o provedení |

| 3 | Testovací proces hlášení (24 hodin/72 hodin) pod vedením | 1 den | O+P: Důkaz o provedení podle § 32/§ 38 |

## 4. Předání a platnost

Tento Kvalifikační posudek obsahuje 20 jednotlivých hodnocení, 5 kompletních balíčků důkazů o provedení a akční plán. Platnost: 12 měsíců nebo do okamžiku prvního spouštěče revalidace (nový cloudový poskytovatel, nové kritické systémy, bezpečnostní incident, podstatná změna v prostředí AV). Po uplynutí této doby či po aktivaci spouštěče rozhodne objednatel znovu, a to bez jakýchkoli závazků a bez stanovení minimální délky smluvního vztahu.

Právní upozornění: Odborná kvalifikace posouzená nezávislým odborníkem. Nejedná se o certifikaci, státní audit ani právní poradenství.

---

VZOR DOKUMENTU PRO DEMONSTRAČNÍ ÚČELY. Nejedná se o skutečný mandát. Název firmy a údaje jsou smyšlené. © CZECURE – Kvalifikace, žádný audit.