

Technické aspekty informačního systému

MONITORING REJSTŘÍKU

Tento dokument shrnuje technické zajištění bezpečnosti osobních údajů v informačním systému

ČÁST PRVNÍ: SEZNAM OSOBNÍCH ÚDAJŮ UCHOVÁVANÝCH V SYSTÉMU MONITORING REJSTŘÍKU

OSOBNÍ ÚDAJE SPRÁVOVANÉ V RÁMCI SYSTÉMU MONITORING REJSTŘÍKU, JE MOŽNO ROZDĚLIT DO DVOU SKUPIN:

a) V rámci systému MONITORING REJSTŘÍKU se pracuje s osobními údaji subjektů, které jsou v rámci služby monitorovány. Mezi tyto údaje patří:

- Název společnosti
- Jméno
- Příjmení
- IČ
- DIČ
- Ulice
- Město
- Telefon
- E-mail
- RČ
- Datum narození

VŠECHNY TYTO ÚDAJE LZE ZÍSKAT Z VEŘEJNĚ PŘÍSTUPNÝCH REJSTŘÍKŮ, A TO:

- Insolvenční rejstřík (ISIR, <https://isir.justice.cz/isir/common/index.do>)
- Administrativní registr ekonomických subjektů (ARES, http://wwwinfo.mfcr.cz/ares/ares_es.html.cz)
- Webová služba pro zjišťování spolehlivosti plátců DPH a bankovních účtů plátců DPH (https://adisspr.mfcr.cz/adistc/adis/idpr_pub/dpr_info/ws_spdph.faces)

b) V systému MONITORING REJSTŘÍKU jsou dále spravovány osobní údaje vztahující se k uživatelským účtům. Mezi tyto údaje patří:

- Jméno
- Příjmení
- Rodné číslo
- IČ
- Telefon
- Email
- Ulice
- Město
- Přihlašovací jméno
- Heslo

Data k uživatelským účtům jsou pořízena a uchovávána na základě platné uživatelské smlouvy.

Podrobný popis datové struktury je definován v technické dokumentaci „OSIRIS-datová-struktura.xls“, která je případně k dispozici dozorovým orgánům.

ČÁST DRUHÁ: DEFINICE PŘÍSTUPŮ K OSOBNÍM ÚDAJŮM V RÁMCI SYSTÉMU MONITORING REJSTŘÍKU

Přístup k datům obsahujícím osobní údaje je možno rozpoznat pro dvě kategorie přístupu.

a) **Uživatelský přístup, tedy přístup zvenčí:**

Přístup k osobním údajům v systému MONITORING REJSTŘÍKU zvenčí je podmíněn autentizací platného uživatele na základě uživatelského jména a hesla. Identifikace a autentizace probíhá v systému MONITORING REJSTŘÍKU. Systém loguje čas a datum přihlášení uživatele do systému pro přístup k datům.

Všechna hesla jsou uchovávána v podobě otisku v nečitelné podobě.

Dotazy do systému jsou logovány a logy prochází pravidelným týdenním vyhodnocením z hlediska správné funkce systému.

b) Administrativní přístup, tedy přístup zevnitř:

Přístup k osobním údajům v systému zevnitř probíhá v rámci údržby systému a poskytování uživatelské podpory, a je vykonáván pouze prověřenými pracovníky, kteří mají přístup k jednotlivým položkám reálných dat, a to pouze v omezeném rozsahu po dobu nutnou v případě nutného technického zásahu.

O těchto přístupech je vedena evidence zásahů a vždy je vyzooměn vlastník – správce osobních dat.

ČÁST TŘETÍ: SEZNAM PLATNÝCH OPERACÍ NAD DATY OBSAHUJÍCÍMI OSOBNÍ ÚDAJE V RÁMCI SYSTÉMU MONITORING REJSTŘÍKU

Nad daty, která obsahují osobní údaje, jsou v systému MONITORING REJSTŘÍKU v rámci provozu funkce prováděny tyto operace:

ČTENÍ DAT

Na data v systému MONITORING REJSTŘÍKU nahlíží výhradně oprávněný uživatel systému, jímž je buď správce dat, anebo jím pověřený zpracovatel dat, a to ve formě webových stránek a informačních mailů.

POŘIZOVÁNÍ DAT

Data do systému MONITORING REJSTŘÍKU vstupují dvěma způsoby:

- manuálním vložením, které je prováděno výhradně validně přihlášeným uživatelem systému, jímž je buď správce dat, anebo jím pověřený zpracovatel dat
- automatickým importem z veřejných zdrojů, tedy z Insolvenčního rejstříku (ISIR), Administrativního registru ekonomických subjektů (ARES) a skrze Webovou službu pro zjišťování spolehlivosti plátců DPH a bankovních účtů plátců DPH

MODIFIKACE

Úpravy dat v systému MONITORING REJSTŘÍKU provádí výhradně validně přihlášený uživatel systému, jímž je buď správce dat anebo jím pověřený zpracovatel dat. Synchronizace se službou Insolvenční rejstřík (ISIR) je prováděna automatizovaně.

MAZÁNÍ DAT

Mazání dat se provádí jejich anonymizací, a provádí ji výhradně validně přihlášený uživatel systému, jímž je buď správce dat, anebo jím pověřený zpracovatel dat.

V případě ukončení poskytování služby MONITORINGU REJSTŘÍKU jsou všechna osobní data v souladu se zákonnými požadavky a lhůtami anonymizována v datovém úložišti. Data se mohou vyskytovat z technických důvodů na záložních médiích po dobu maximálně 3 měsíců od ukončení smlouvy se správcem dat.

EXPORT DAT

Export dat provádí poskytovatel systému na žádost správce dat.

ULOŽENÍ DAT

Všechna data, která jsou uložena v MONITORING REJSTŘÍKU jsou fyzicky umístěna na dedikovaných serverech umístěných v datovém centru společnosti ZONER software, a.s. v České republice.

Servery využívané společností Insolvence 2008, a.s. jsou spravovány společností ZONER software, a. s.

- Prohlášení o ochraně soukromí ve společnosti ZONER software, a.s. <https://www.czechia.com/clanek/ochrana-soukromi/>
- <https://www.czechia.com/clanek/technicke-aspekty-zabezpeceni-osobnich-udaju-u-zpracovatele-zoner-software/>

Detailní popis serverů a rozdělení služeb mezi ně je definován v technické dokumentaci „ISIS a Osiris servery“, která je případně k dispozici dozorovým orgánům.

Všechny provozované webové služby na výše uvedených serverech jsou zprostředkovány výlučně zabezpečeným protokolem HTTPS .

Ochrana serverů a celé infrastruktury je zajišťována společností ZONER software, a. s.

Na serverech je provozován operační systém Linux v aktuálních verzích.

Servery jsou virtuální, běžící na platformě VMware. Certifikace dané platformy viz <http://www.vmware.com/cz/security/certifications.html>.

ZÁLOHOVÁNÍ

Všechny databáze a úložiště dokumentů jsou denně zálohovány prostřednictvím zálohovacích procesů správce serverového řešení společnosti ZONER software, a. s.

DOBA ARCHIVACE

Dobu archivace si určuje správce dat.

VÝVOJ SOFTWARE

Vývoj systému MONITORING REJSTŘÍKU probíhá na anonymních datech. Pracovníci vývojového oddělení a technické podpory osobní data nezpracovávají ani nemodifikují. Pouze pověřeni pracovníci mají přístup k jednotlivým položkám reálných dat, a to omezeně a pouze v případě nutného technického zásahu. O těchto přístupech je vedena evidence zásahů a vždy je vyrozuměn vlastník – správce osobních dat.

Z výše uvedeného je průkazné, že MONITORING REJSTŘÍKU má všechny funkce, které jsou nezbytné k zajištění ochrany práv subjektu údajů. Správce, který si zvolil MONITORING REJSTŘÍKU, splnil tuto povinnost uvedenou v článku 27 odst. 1 obecného nařízení EU o ochraně osobních údajů 2016/679.