

**ZADAVATEL: RYANT, s.r.o., IČ: 262 49 871, SPOLEČNOST SE SÍDLEM
KOTKOVA 20, 670 25 ZNOJMO**

V PRAZE DNE 26. DUBNA 2006

**ANALÝZA DOPADŮ USNESENÍ VLÁDY ČESKÉ
REPUBLIKY Č. 624/2001 A DALŠÍCH PRÁVNÍCH PŘEDPISŮ
NA UŽÍVÁNÍ PRODUKTU RYANT SOFTWARE AUDIT
ORGÁNY STÁTNÍ A VEŘEJNÉ SPRÁVY**

**ZPRACOVATEL: JUDR. KLÁRA VESELÁ – SAMKOVÁ, ADVOKÁTKA
Č. REG. U ČAK 3005
SE SÍDLEM ŠPANĚLSKÁ 6, 120 00 PRAHA 2**

I. VÝCHOZÍ STAV

Zadavatel je původcem a vlastníkem majetkových práv k software – produktu s názvem RYANT Software Audit (dále jen „RSA“). RSA je programovým nástrojem, který uživateli umožňuje získat prostřednictvím tohoto produktu přehled o využití jednotlivých aplikací na HW vybavení uživatele, využití pracovní doby zaměstnanců (přehled o využívání jednotlivých pracovních stanic na pracovišti, využití času apod.) a inventarizaci software a hardware v rámci počítačové sítě uživatele. Zadavatel RSA poskytuje buď formou licence na software – tj. software je instalován na hardware uživatele, nebo formou poskytnutí služby. V případě varianty poskytnutí Služby RSA uživatel nenabývá uživatelská práva k software, RSA je v tomto případě prostředkem v rukou Zadavatele s jehož pomocí dodává Zadavatel v rámci časově omezeného smluvního vztahu uživateli výstupy – analýzu dle zadání příslušné smlouvy.

Zadavatel požaduje posouzení dopadů Usnesení vlády České republiky č. 624/2001, případně dalších právních předpisů České republiky a aplikovatelných norem Evropské unie na užívání RSA jednotlivými subjekty, s důrazem na subjekty z oblasti veřejné a státní správy.

II. DOPADY USNESENÍ VLÁDY ČR ZE DNE 20. 6. 2001 Č. 624+P

1. **Usnesením Vlády České republiky č. 624/2001 (dále jen „Usnesení“)** vláda zejména schvaluje Pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů jako závazný dokument pro orgány státní správy a jimi řízené organizace. Účelem tohoto dokumentu je stanovit transparentní, komplexní a jednotný systém pravidel pro kontrolu užívání počítačových programů v souladu s platnými právními předpisy a příslušnými licenčními ujednáními, a to stanovením základních podmínek pro nabývání, instalaci a užívání počítačových programů a stanovením zásad a způsobu zabezpečení pravidelných kontrol užívání počítačových programů a stanovením zásad a způsobu zabezpečení pravidelných kontrol užívání počítačových programů na všech ministerstvech a ostatních orgánech státní správy, včetně v jimi řízených organizacích.

2. Usnesení stanovuje několik zásadních pravidel pro pořizování a užívání počítačových programů:

a) **Požadavek legality software:** počítačové programy musí být pořizovány důsledně v souladu s autorským zákonem, tj. v rámci pořizování software nesmějí být porušena práva třetích osob. *Vzhledem k tomu, že Zadavatel je přímo původcem software, budou licence k RSA vždy licencemi legálními, Zadavatel má k poskytovanému RSA neomezené dispoziční právo. Standardní smluvní dokumentace Zadavatele obsahuje transparentní licenční podmínky specifikující rozsah uživatelského práva užití software a je dostatečným podkladem pro prokázání oprávněnosti používání počítačového programu ve smyslu ustanovení čl. 4 Usnesení. V případě Služby RSA není software instalován na HW uživatele, uživatel nabývá na základě příslušné smlouvy práva k finálnímu výstupu – objednané analýze.*

b) **Požadavky na dokumentaci oprávněnosti užívat počítačové programy a jejich evidenci:** jako základní doklad o oprávněnosti použití programu slouží dle Usnesení zaplacená faktura (*pravděpodobně měl autor Usnesení na mysli vystavenou fakturu a doklad o jejím uhrazení*). Dále usnesení stanoví demonstrativní výčet dokumentace, kterou lze prokázat užívací titul k programovému vybavení. Usnesení stanovuje požadavky na vedení evidence o instalaci počítačových programů, o jejich vyřazení a o převodu práv k užívání počítačových programů.

Standardní smluvní dokumentace Zadavatele obsahuje veškerou požadovanou agendu, s jejíž pomocí je uživatel schopen prokázat oprávněnost použití programového vybavení. Jednou ze základních funkcionalit RSA je inventarizace hardwarového a softwarového vybavení bez ohledu na jejich používání. RSA může být proto používán i jako nástroj k dodržení evidenčních a inventarizačních povinností stanovených v čl. 5 Usnesení, a to jak v případě poskytnutí licence RSA, tak v případě Služby RSA .

c) **Požadavek na zajištění oprávněnosti užívání počítačových programů:** Povinné subjekty musí zajistit dodržování platných právních předpisů týkajících se nakládání s počítačovými programy a dodržování licenčních smluv. Nakládání s počítačovými programy podléhá zejména regulaci

zákona č. 121/2000 Sb., autorského zákona. *Povaha RSA, skutečnost, že Zadavatel je původcem programu, a povaha dodávané standardní dokumentace je na straně Zadavatele v naprostém souladu s požadavky autorského zákona.*

III. SOULAD RSA S DALŠÍMI PRÁVNÍMI PŘEDPISY NA ÚZEMÍ ČR:

- **Listina základních práv a svobod** (2/1993 Sb.) - čl. 13. stanoví „Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“ Další rozšiřující výklad k tomuto tématu dodává **Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.** Uvozovací článek (24) k této Směrnici stanoví: „Koncové zařízení uživatelů sítí elektronických komunikací a jakékoli informace uchovávané na takovém zařízení tvoří součást soukromí uživatelů, které vyžaduje ochranu v souladu s Evropskou úmluvou na ochranu lidských práv a základních svobod. Tzv. špehovací software ("spyware"), webové štěnice ("web bugs"), skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí, s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů by mělo být povoleno pouze k oprávněným účelům a s vědomím uživatelů, kterých se dotýká.“ **Úřad na ochranu osobních údajů ve svém stanovisku č. 1/2003 o monitorování elektronické pošty a ochraně soukromí zaměstnanců** citovanou směrnici vykládá s tím, že zaměstnanec má skutečně právo očekávat přiměřenou ochranu soukromí na pracovišti, nicméně toto právo musí být realizováno v maximálním souladu s právy a oprávněnými zájmy zaměstnavatele. Úřad dále uvádí: „Zaměstnavatel má právo sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Pro výkon tohoto práva nemá zaměstnavatel právo sledovat, monitorovat a zpracovávat obsah korespondence svých zaměstnanců. Zaměstnavatel by případně mohl pouze

sledovat počet e-mailů došlých a odeslaných u svých zaměstnanců a požadovat, aby své soukromé záležitosti v pracovní době a na pracovišti vyřizovali v přiměřené a více méně v nezbytné míře, neboť, jak bylo výše uvedeno, ani pracovněprávní vztah neodstraňuje právo na přiměřené soukromí zaměstnanců. O svém záměru či praxi sledovat četnost přijímaných či odesílaných e-mailových zpráv by měl zaměstnavatel předem své zaměstnance uvědomit, a to nejlépe při navazování pracovního vztahu. K uvedenému účelu by měla existovat obecná pravidla pro zaměstnavatele a zaměstnance, z nichž by mělo být jasné, že obsah pošty je chráněn a že ve vztahu k němu se ctí listovní tajemství i ochrana osobních údajů.“ *Funkcionalita RSA fakticky neporušuje žádným způsobem tajemství dopravovaných zpráv. RSA je schopno rozlišit, že se zaměstnanec pohybuje v programech pro elektronickou poštu nebo na internetových aplikacích pro elektronickou poštu – internetových schránkách; RSA je schopno identifikovat předmět zpráv. Tato úroveň detailu nenarušuje soukromou sféru subjektu ani vnitřní integritu dopravované zprávy. Zadavatel by měl doporučit uživateli přijmout taková opatření, aby zaměstnanci měli po celou dobu pracovního poměru prokazatelným způsobem k dispozici informaci o tom, že zaměstnavatel může osobně nebo pomocí technických prostředků kontrolovat využití pracovní doby a svěřených prostředků na straně zaměstnanců. Z praxe se nejlépe osvědčuje oznámení v rámci interní směrnice upravující bezpečnost a užívání informačních technologií na pracovišti.*

- **Zákon č. 65/1965 Sb., Zákoník práce**, stanovuje v §73 odst. 1 povinnost zaměstnanců „plně využívat pracovní doby a výrobních prostředků k vykonávání svěřených prací, plnit kvalitně, hospodárně a včas pracovní úkoly“ a „řádně hospodařit s prostředky svěřenými jim zaměstnavatelem ... a nejednat v rozporu s oprávněnými zájmy zaměstnavatele.“ Zároveň je v § 74 stanovena povinnost vedoucích zaměstnanců „řídít a kontrolovat práci a pravidelně hodnotit poměr zaměstnanců k práci a k pracovnímu kolektivu a jejich pracovní výsledky“ a „zabezpečovat přijetí včasných a účinných prostředků k ochraně majetku zaměstnavatele“. *Lze konstatovat, že RSA je produktem vytvořeným pro účely realizace citovaných paragrafů zákoníku práce. S ohledem na výše uvedená omezení tohoto práva a povinnosti v rámci pracovněprávních vztahů (přiměřenost zásahu*

do soukromé sféry zaměstnanců), je nutno i v této souvislosti přijmout příslušná interní opatření na straně uživatele (informace o možnosti kontroly v rámci interních směrnic nebo pracovního řádu uživatele). Nutno ovšem zdůraznit, že zákoník práce nevylučuje použití technických prostředků pro monitorování a vyhodnocování pracovních návyků zaměstnanců. V každém konkrétním případě je však nutné aplikovat požadavek přiměřenosti. Na druhé straně, paušálním odmítnutím „monitorování“ činnosti zaměstnanců s ohledem na ochranu soukromí dle občanského zákoníku a Listiny bychom se dostali do přímého rozporu s požadavky jiných právních předpisů – například zákoníku práce nebo předpisů BOZP. Tímto způsobem bychom také prohlásili za nezákonné např. „píchačky“ monitorující příchod pracovníků do zaměstnání, nebo elektronické karty, které poskytují výstupy o pohybu zaměstnanců po pracovišti, které jsou dnes považovány za normální a standardní bezpečnostní a kontrolní mechanismy.

- Nelze též opomenout trestněprávní odpovědnost zaměstnavatelů (statutárních orgánů a vedoucích zaměstnanců) za to, jakým způsobem je nakládáno s koncovými zařízeními v majetku zaměstnavatele. Zaměstnavatel je proto i z tohoto ohledu důsledně povinen kontrolovat, zda na koncových zařízeních nedochází například k užívání nelegálního software, stahování nelegální hudby a filmů (porušování autorských práv třetích osob) nebo např. k šíření pornografie.
- V souvislosti s aplikací zákona 65/1965 Sb., zákoníku práce je třeba též upozornit na §1 zákoníku práce, který detailně definuje diskriminační jednání. RSA poskytuje uživateli takové výstupy, které mohou být uživatelem dále používány v rozporu s platným právním řádem ČR. Např. se uživatel může prostřednictvím RSA dozvědět, že jeho zaměstnanec navštěvuje z firemního počítače webové stránky s homosexuální tematikou. Na základě této informace propustí uživatel zaměstnance z práce a dopustí se tak diskriminačního jednání dle §1 zákoníku práce, přičemž diskriminační nejsou výstupy z RSA, ale následné rozhodnutí uživatele. **Zadavatel nemůže ovlivnit způsob, jakým uživatel dále naloží s výstupy RSA. Příslušné analýzy umožňují detailní selekci analyzovaných dat; Zadavatel nemůže ovlivnit ani odpovídat za to, zda na základě zjištění učiněných prostřednictvím RSA neučiní uživatel taková rozhodnutí nebo**

opatření, která budou napadena jako diskriminační. Doporučujeme proto, aby byli uživatelé upozorněni v rámci proškolení nebo poskytování výstupů k RSA na dopad antidiskriminačních norem českého právního řádu na aplikaci příslušných výstupů, s důrazem na ustanovení Zákoníku práce a Listiny základních práv a svobod .

- **Zákon č. 127/2005 Sb., zákon o elektronických komunikacích** – nevztahuje se dle našeho názoru přímo na RSA, Zadavatel není podnikatelem poskytujícím veřejně dostupnou službu elektronických komunikací. §89 odst. 1 tohoto zákona stanoví: „Podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti.“ *Nelze vyloučit, že v případě soudního sporu bude toto ustanovení používáno v rámci výkladu k citovanému ustanovení Listina jako anlogia iuris. Přesto i zde platí, že RSA nenarušuje důvěrnost přepravovaných dat a úroveň detailu informace, kterou zpřístupňuje uživateli, naplňuje základní požadavek přiměřenosti ve vztahu k ochraně soukromí zaměstnanců uživatele.*

IV. ZÁVĚR

Produkt Zadavatele s názvem RYANT Software Audit, ať již poskytovaný formou licence k software nebo jako služba, jejímž výstupem jsou uživatelem požadované analýzy, byla a je společností RYANT s.r.o. – původcem a vlastníkem majetkových práv k RSA – vyvinuta a distribuována **v souladu s platným právním řádem České republiky**. Produkt RSA vyhovuje jak kritériím zákona autorského, tak požadavkům Usnesení vlády České republiky č. 624/2001, ostatních právních předpisů i relevantních norem Evropské unie. Standardní smluvní dokumentace uzavíraná Zadavatelem je dostatečně určitá a průkazná pro prokázání patřičných práv uživatele k RSA, ať již ve formě licenčních práv nebo výstupů služby RSA.

Zadavatel by měl doporučit uživatelům, aby do svých interních směrnic nebo do uzavíraných pracovních smluv inkorporovali upozornění svým zaměstnancům, že zaměstnavatel může formou kontrol i pomocí technických prostředků kontrolovat využití pracovní doby a pracovních prostředků ze strany zaměstnanců. Inkorporováním takového upozornění do interních směrnic se uživatel vyvaruje jakýmkoli pozdějším problémům, neboť tento postup je v souladu i s nejstriktnějšími výklady evropské legislativy.

Zadavatel také nemůže ovlivnit způsob, jakým uživatel dále naloží s výstupy RSA. Příslušné analýzy umožňují detailní selekci analyzovaných dat; Zadavatel nemůže ovlivnit ani odpovídat za to, zda na základě zjištění učiněných prostřednictvím RSA neučiní uživatel taková rozhodnutí nebo opatření, která budou napadena jako diskriminační. Doporučujeme proto, aby byli uživatelé upozorněni v rámci proškolení nebo poskytování výstupů k RSA na dopad antidiskriminačních norem českého právního řádu na aplikaci příslušných výstupů, s důrazem na ustanovení Zákoníku práce a Listiny základních práv a svobod .