

1 0 1 0 1 0 0 1 1 1 0 0 0 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 1 1 0 1 1 0 0

Nařízení o ochraně osobních údajů

GDPR – GENERAL DATA PROTECTION REGULATION



Magazín GDPR

číslo 4/2019



... Máme řešení i pro Vaši společnost

www.softbit.cz

Vážení uživatelé našich informačních systémů,

pro všechny naše uživatele jsme připravili nové číslo našeho nepravidelného magazínu věnovaného tématice ochrany osobních údajů podle GDPR. Načerpali jsme další poznatky, které si myslíme, že budou pro Vás přínosné.

V řadě případů čerpáme přímo z informací uvolněných Úřadem pro ochranu osobních údajů doplněných o naše poznámky.

Věříme, že pro Vás informace, které získáte díky našemu dalšímu magazínu, budou užitečné při lepším zajištění procesů v ochraně osobních údajů ve Vaší organizaci podle GDPR.

**Přejeme
Vám příjemné
čtení**



Bc. Dana Peremská
pracovník zákaznické podpory

Obsah magazínu

Nabídka služeb GDPR

Jak zrevidovat dokumentaci

Pokuta od ÚOOÚ – zohlednění konkrétní okolnosti

GDPR a cloud

NA ZÁVĚR

Tým společnosti Softbit Software s.r.o

4

5

7

10

13

14

Nabídka služeb GDPR

Naše společnost rozšířila v roce 2017 nabídku o poskytování služeb v oblasti správy a ochrany osobních údajů. V současné době naše služby v této oblasti využívá více jak 100 zákazníků z různých oblastí státní správy i podnikatelského světa.

V loňském roce jsme se všemi zákazníky v oblasti GDPR zpracovali základní pravidla pro ochranu a správu osobních údajů fyzických osob včetně školení odpovědných pracovníků v jednotlivých organizacích a společnostech.

Vzhledem k tomu, že téma ochrany osobních údajů fyzických osob se neustále vyvíjí, ani naše společná práce v této oblasti by neměla skončit. Jak víte, letos v dubnu naši zákonodárci konečně schválili Adaptační zákon číslo 110/2019 Sb., který upravuje část problematiky v ochraně osobních údajů podle nařízení GDPR. Připravili jsme proto pro Vás nabídku pro aktualizaci opatření pro ochranu osobních údajů právě ve Vaší společnosti či organizaci.

Nabídka našich služeb GDPR na léto 2019 obsahuje tyto služby:

Aktualizace směrnice

Nabízíme aktualizaci směrnice podle Českého adaptačního zákona a aktuálních výkladů nařízení GDPR. Aktualizovanou směrnici Vám předáme v tištěné i elektronické podobě.



Revize

Provedeme revizi všech činností spojených s ochranou a správou osobních dat. Zkontrolujeme opatření, která byla provedena v souvislosti se zavedením ochrany osobních údajů podle GDPR. O výsledku revize pro Vás sestavíme zprávu.



Školení pracovníků

Dále nabízíme individuální školení pro pracovníky organizace či společnosti v ochraně osobních údajů fyzických osob se zaměřením na aktuální stav legislativy a upozorníme na nejčastější chyby.

Ceník služeb GDPR

Aktualizace směrnice GDPR pro rok 2019	od 1.900,- Kč včetně zaslání nové směrnice v tištěné podobě
Revize	900,- Kč/hod
Školení pracovníků	1.200,- Kč/hod
Konzultace pověřence pro ochranu osobních dat pana Tomáše Urbana	900,- Kč/hod

Ceny nezahrnují cestovní výdaje a jsou uvedeny bez DPH 21 %.

Jak zrevidovat dokumentaci

Po schválení Adaptačního zákona č. 110/2019 Sb., o zpracování osobních údajů, je **nutné provést revizi dokumentace** upravující zpracování osobních údajů v organizaci. Tuto revizi je důležité provést zejména tam, kde dokumenty odkazovaly na předchozí zákon o ochraně osobních údajů č. 101/2000 Sb. Ačkoliv se změny vzniklé účinností Adaptačního zákona mohou zdát nepodstatné, doporučujeme nepodcenit revizi dokumentace. Revize je vhodná pro zhodnocení dopadů GDPR za uplynulý rok na provoz organizace a také je vhodná k nápravě případných nedokonalostí.

**Nepodceňujte
revizi
dokumentace
GDPR**

**Věková
hranice
nezletilých**

Věková hranice pro udělení souhlasu se zpracováním údajů u nezletilých osob je **nově stanovena na 15 let**. Je tedy vhodné, aby organizace, ve kterých dochází ke zpracování osobních údajů nezletilých osob, a to v souvislosti s nabídkou služeb informační společnosti (online), **zrevidovali stávající podobu souhlasů a nastavení věkové hranice**, od níž je nezletilý oprávněn k udělení souhlasu se zpracováním údajů.

Nejedná se pouze o formální úpravu v dokumentaci a případnou změnu věkové hranice. Je třeba provést procesní opatření, jehož pomocí správce během získávání souhlasu přiměřeným způsobem ověří, že subjekt údajů dané věkové hranice dosáhl. Toto procesní opatření je však z praktického hlediska problém v případě udělení souhlasu přes internet, jelikož správce údajů má značně omezené možnosti ověření identity subjektu údajů, aniž by se vyvaroval nepřiměřeně složitého a administrativně náročného procesu získávání souhlasu. Pro zjištění dosažení věkové hranice k udělení souhlasu bude rozhodující, zda se jedná o službu určenou primárně pro děti/nezletilé nebo se jedná o službu k oprávněnému užití nezletilými osobami, ale bez primárního určení pro ně. V tomto případě nelze klást na správce nepřiměřené požadavky na ověřování dosažení věkové hranice.

**Procesní
opatření**

**zjištění
dosažení věkové
hranice**

**ust.
§ 10 zákona č.
110/2019 Sb.**

Nově podle ust. § 10 zákona č. 110/2019 Sb., o zpracování osobních údajů, **nemusí správce provádět posouzení vlivu** na ochranu osobních údajů před zahájením nové operace jejich zpracování, pokud mu jiný právní předpis stanoví povinnost takové zpracování osobních údajů provést. Je tedy nutné upravit dokumentaci i v této oblasti. Jestliže správce vyhodnotí, že určité operace zpracování musí provádět ze zákona, je dobré do dokumentace k GDPR uvést, o jaké typy zpracování údajů se jedná a z jakého důvodu je provádí (nejlépe s odkazem na příslušná ustanovení konkrétního zákona).

**zákon č.
253/2008 Sb.**

Podle zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, musí řada tzv. povinných osob provádět identifikaci subjektů údajů (často v postavení klienta) v širokém rozsahu, včetně rodného čísla nebo čísla identifikačního dokladu. Tímto zákonem tedy odpadá nutnost provádět posouzení vlivu na ochranu údajů. Povinností správce je identifikace, musí tedy zpracovat údaje. V daném případě je pak nezbytné pouze nastavit přiměřená bezpečnostní a procesní opatření k zajištění bezpečnosti údajů.

ust.
§ 47 zákona č.
110/2019 Sb.

Dle nového ust. § 47 zákona č. 110/2019 Sb., o zpracování osobních údajů, je **mlčenlivost zaměstnanců** v oblasti osobních údajů, s nimiž se dostanou do kontaktu **zařazena v Hlavě IV** zákona, jež pojednává o ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů ČR.

zákon č.
111/2019 Sb.

S účinností zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, došlo k dílčím změnám některých zákonů. Je nutné posoudit, zda na konkrétního správce či zpracovatele osobních údajů dopadají i tyto dílčí změny některých zákonů. Změny se týkají pouze specifických správců, a to sektor civilního letectví, notáři, advokáti, justice, Česká národní banka nebo policie.

Pro některé veřejné orgány se upřesňují pravidla pro stanovení pozice pověřence, avšak i ty nejsou pro většinu správců podstatné (především pro správce ze soukromého sektoru).

správní
řád a občanský
soudní řád

Další změny s účinností Adaptačního zákona se nacházejí ve správním řádu nebo v občanském soudním řádu. Ve věcech ochrany osobních údajů se subjekt údajů může v řízení dát zastupovat i právnickou osobou, jejíž zisk se nerozděluje a k jejímž činnostem uvedeným v zakladatelském právním jednání patří ochrana práv subjektů údajů. V takových případech za právnickou osobu jedná pověřený zaměstnanec nebo člen, který má vysokoškolské právnické vzdělání, jež se podle zvláštních předpisů vyžaduje pro výkon advokacie.

Pokuta od ÚOOÚ – zohlednění konkrétní okolnosti

Úřad pro ochranu osobních údajů (dále jen ÚOOÚ) vždy při stanovení výše pokut za porušení GDPR zohledňuje konkrétní okolnosti případu. Zohlednění konkrétních okolností případu představuje, že se uplatní princip individualizace správních pokut. Výčet okolností, které dozorový úřad musí při ukládání pokuty v konkrétním případě zohlednit, lze nalézt v čl. 83 odst. 2 GDPR.

čl. 83 odst. 2
GDPR

Povaha,
závažnost,
délka trvání

Příkladem lze uvést povahu, závažnost a délku trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena, o kroky podniknuté správcem nebo zpracovatelem ke zmírnění škod způsobených subjektům údajů, o kategorie osobních údajů dotčených daným porušením či o způsob, jakým se dozorový úřad o porušení dozvěděl, zejména zda a v jaké míře správce nebo zpracovatel porušení oznámil.

Polehčující a přitěžující okolnosti se mohou projevovat před spácháním přestupku, v průběhu páchaní přestupku nebo i po spáchání přestupku.

Níže jsme pro Vás vybrali několik příkladů z praxe, ve kterých se můžete dočíst, jaká okolnost je polehčující a jaká Vám naopak přitíží.

Příklady okolností zvyšující a snižující závažnost porušení GDPR:

Ve věci č. j. UOOU-00178/19 porušila společnost zásadu zákonnosti, korektnosti a transparentnosti tím, že subjekty údajů neinformovala o zpracování osobních údajů prostřednictvím GPS lokátorů, jež byly umístěny ve vozidlech, a dále o totožnosti a kontaktních údajích správce osobních údajů, o účelech zpracování, pro které jsou osobní údaje určeny, a právním základu pro zpracování, o době uložení osobních údajů atd.

zvýšení
závažnosti

ÚOOÚ přihlédl při stanovení sankce k absolutnímu neplnění povinnosti týkající se transparency ve vztahu ke zpracování osobních údajů prostřednictvím GPS lokátorů.

snížení
závažnosti

ÚOOÚ přihlédl k tomu, že správce během kontroly spolupracoval a činil kroky k nápravě protiprávního stavu.

Ve věci č. j. UOOU-09571/18-14 nezajistil správce osobní údaje přibližně 300 svých klientů v rozsahu jméno, příjmení, rodné číslo, číslo OP, adresa bydliště, telefonní číslo a informace o úvěru, které byly obsaženy ve smlouvách o spotřebitelském úvěru, byly volně uloženy v papírové krabici v prostorách společných garáží bytového domu minimálně po dobu 14 dnů a následně nalezeny v kontejneru.

zvýšení
závažnosti

Osobní údaje se týkaly většího počtu subjektů údajů. Nalezené listiny obsahovaly také rodná čísla, která slouží jako obecný identifikátor občanů. Správce v rámci ohlášení porušení zabezpečení uvedl hrubě zavádějící informaci týkající se počtu odcizených dokumentů s osobními údaji (ohlásil ztrátu přibližně 80 smluv, ale ve skutečnosti šlo o více než 300 klientů).

snížení závažnosti

Správce přijal opatření, aby zamezil opětovnému porušení povinnosti uložené zákonem, a rovněž k jeho majetkovým poměrům.

Ve věci č. j. UOOU-00163/19-3 se jednalo o neuzavření zpracovatelské smlouvy se zpracovatelem osobních údajů a nedodržení zásady integrity a důvěrnosti, tedy nezajištění osobních údajů hráčů internetové online hry, a to v rozsahu hráčské jméno, heslo k hernímu účtu, ID herního účtu, e-mailová a IP adresa, v důsledku čehož došlo mimo jiné ke zveřejnění těchto údajů na internetu po dobu přibližně 30 minut.

zvýšení závažnosti

Porušení více povinností a únik osobních údajů více hráčů.

snížení závažnosti

Správce učinil kroky směřující k následnému zabezpečení zpracování osobních údajů a současně kroky, jejichž cílem bylo informovat dotčené subjekty údajů a poučit je, jak mají dále postupovat.

Ve věci č. j. UOOU-08244/18-15 zaměstnavatel zveřejňoval od roku 2017 do ledna roku 2019 prostřednictvím Facebook na svém profilu osobní údaje bývalé zaměstnankyně v rozsahu jméno, příjmení, titul a fotografie, a to i přes opakovanou výzvu k jejich odstranění.

zvýšení závažnosti

Správce zveřejnil osobní údaje prostřednictvím internetu, tedy v podstatě neomezenému počtu příjemců. Údaje nevymazal ani po výzvě dotčeného subjektu údajů a ani po opakované výzvě ÚOOÚ.

snížení závažnosti

Jestliže je počet dotčených subjektů údajů nízký, může se jednat o okolnost snižující závažnost jednání.

Ve věci č. j. UOOU-02062/19-3 došlo k nezákonnému zpracování osobních údajů v rozsahu jméno, příjmení, rodné číslo, datum narození, pohlaví, místo narození, občanství, adresa trvalého pobytu, číslo OP včetně jeho platnosti a úřadu, který ho vydal, s cílem neoprávněně a účelově založit běžný účet osobě, jež byla disponentem jiného účtu, a to bez jejího vědomí.

zvýšení závažnosti

Protiprávní jednání trvalo delší dobu (přibližně 1 rok a 5 měsíců). Správce je bankou, tedy profesionálem v oboru, kde dochází k rozsáhlému zpracování osobních údajů. Jednáním správce bylo porušeno více povinností stanovených GDPR.

snížení závažnosti

Porušení povinnosti bylo prokázáno pouze u jedné dotčené osoby.

Ve věci č. j. UOOÚ-07108/18-11 došlo k porušení čl. 15 odst. 1 GDPR. Jednalo se o neposkytnutí informace o zpracování osobních údajů subjektu údajů, a to i přes jeho žádost.

**zvýšení
závažnosti**

Bylo porušeno jedno ze základních práv, které subjektu údajů slouží k tomu, aby mohl posoudit zákonnost procesu zpracování jeho osobních údajů, tedy transparentnost a korektnost zpracování. Správce neumožnil subjektu údajů přístup k jeho osobním údajům ani po opakované výzvě ÚOOÚ.

**snížení
závažnosti**

Protiprávním jednáním byl dotčen pouze jeden subjekt údajů.

ÚOOÚ hledí na:

- ✓ počet dotčených subjektů údajů
- ✓ zda a jak správce reaguje na výzvy subjektu údajů a ÚOOÚ
- ✓ jak správce spolupracuje s ÚOOÚ během kontroly
- ✓ délku trvání porušení (kdy délka 3 měsíce není dostatečná a není tedy brána jako polehčující okolnost; naopak 1 rok a 5 měsíců je hodnoceno jako okolnost přitěžující)
- ✓ porušení čl. 15 odst. 1 GDPR je přitěžující okolnost

Více o zmíněných příkladech si můžete přečíst na stránkách [Úřadu pro ochranu osobních údajů](#).

GDPR a cloud

Na co se zaměřit při výběru cloudu

V minulém čísle našeho magazínu GDPR jsme Vás informovali co je cloud, co je jeho výhodou a jaký má vztah k GDPR. V tomto článku si řekneme, jak vybrat vhodného poskytovatele cloudu a na co se při jeho výběru zaměřit.

V tabulce uvedené níže jsou vybrány požadavky a možná opatření na zabezpečení dat.

Požadavek na zabezpečení dat	Rozbor situace v cloudu	Možná opatření
Přístupová práva a bezpečný přístup	➔ Je nutné zajistit, aby se každý zaměstnanec firmy dostal pouze k těm uloženým datům, která se ho týkají. ➔ Kontrola reálně nastavených práv je však ve veřejném cloudu téměř nemožná. V dnešní době je možné se do 25 % obsahu ve světových veřejných cloudech dostat i bez znalosti hesla (např. sdílením fotografií). ➔ V privátním cloudu je nutné zajistit přístup vlastního administrátora, který uvidí na práva a případně je bude měnit. Také je potřeba ošetřit přístupy alespoň administrátorů poskytovatele (např. smlouvou o mlčenlivosti).	✓ Využít všechny dostupné možnosti silné autentizace (např. dvoufaktorová autentizace – přihlášení heslem a PIN kódem) ✓ V případě privátního cloudu je potřeba zajistit možnost administrace vlastní organizací a sběr logů. ✓ Doporučuje se také zjistit počet osob poskytovatele s možným přístupem k datům a ošetřit smluvně sankce pro případ úniku dat.
Vhodná aplikace	➔ Aplikace v cloudu nemá žádné nevýhody ➔ Problémem jsou chyby v zabezpečení proti hackerským útokům. Vzniká tak velká zranitelnost, která může být zneužita dříve, než by hrozilo v podnikové síti.	✓ Ochrana závisí na dodavateli/programátorovi aplikace. ✓ Mělo by být ošetřeno smluvně, že aplikace vyhoví požadavkům GDPR. ✓ Doporučuje se provádět penetrační testy cloudového prostředí, které by měly odhalit případnou zranitelnost.
Šifrování a uložení dat	➔ V současné době již většina cloudů používá k zaslání dat na cloud nebo z cloudu protokol HTTPS, který je považován za bezpečný. ➔ Problémem je poskytování dat. Poskytovatelé cloudu tvrdí, že data různých organizací v cloudu jsou od sebe striktně oddělena. Pro administrátory toto však neplatí. ➔ V privátním cloudu se doporučuje zajistit, aby byla data uložena na samostatném fyzickém serveru.	✓ Zda jsou data na cloud posílány prostřednictvím HTTPS:// je vidět přímo v adresním řádku internetového prohlížeče. ✓ Nejlepší je v každém případě ukládat v cloudu pouze data předem šifrovaná organizací. To však nelze zajistit (např. v případě aplikace používané v cloudu, pokud s šifrováním nepočítá).
Zabezpečení proti síťovým útokům	➔ Cloud je napadán hackery více než podnikové prostředí. Zabezpečení pomocí firewallů, proxy atd. by mělo být samozřejmostí. ➔ V případě veřejného cloudu často nevíme, zda cloud obsahuje ochranné prvky a na jaké úrovni. ➔ V případě privátního cloudu lze sjednat ochranné prvky, avšak nemáme k dispozici jejich nastavení ani logy z jejich činnosti. ➔ Hackery je dobré zablokovat již prostřednictvím firewallu. ➔ Vnitřní síťové útoky se doporučuje v rámci cloudu neřešit. Největší hrozbu pro data na vnitřní síti cloudu představují administrátoři poskytovatele, a ti si přístup mohou získat prostřednictvím přístupových práv (i bez síťových útoků).	✓ Zda je na cloudu nastaven firewall a jaký typ lze v některých případech ověřit i u veřejného cloudu. Nelze však ověřit, zda tomu tak skutečně je. ✓ V případě privátního cloudu lze nasadit vlastní firewall nebo sjednat možnost posílání na vyžádání nastavení firewallu a logy z něj.

Škodlivé kódy

- Na veřejném cloudu je často intenzivní provoz z internetu. Veřejný cloud je tedy více napadán a pravděpodobnost zavirování je velká. - Zabezpečení antivirovým programem by mělo být samozřejmostí. Především, aby nedošlo k poškození či zničení uložených osobních údajů. - V případě veřejného cloudu obvykle nevíme, jestli cloud antivir obsahuje a na jaké úrovni. V některých případech lze další ochranu proti malwaru sjednat za poplatek. - V případě privátního cloudu lze antivir sjednat nebo dodat vlastní. Většinou však nemáme k dispozici aktuální nastavení antiviru ani logy z jeho činnosti.	- Zda je na cloudu nastaven antivir a jaký typ lze v některých případech ověřit i u veřejného cloudu. Nelze však ověřit, zda tomu tak skutečně je. - Jestliže si lze připlatit za dodatečnou antivirovou ochranu, doporučujeme si ji vždy sjednat. - V případě privátního cloudu lze nasadit vlastní antivir nebo sjednat možnost posílání na vyžádání nastavení antiviru a logy z něj.
---	---

Fyzický přístup

Nikdy není možné ověřit, zda se k serverům a úložištím nemohou fyzicky dostat další osoby, o nichž nic nevíte.	- V případě veřejného cloudu ani nevíme, kde všude jsou naše data fyzicky umístěna. - V případě privátního cloudu lze někdy sjednat zaslání záznamu z kamer nebo instalovat vlastní kamery, pokud jsou však data umístěna fyzicky samostatně. - Jedná se o jeden z důvodů, proč je lepší hosting v samostatném fyzickém stroji než ve virtuálním prostředí společném s více firmami. - Stejně je však velmi obtížný 24hodinový monitoring kamery.
--	--

Monitoring provozu a sběr logů

- Ačkoliv poskytovatel tvrdí existenci dohledových center, sběrů logů do SIEMu atd. není to pro Vaše potřeby, ale pro potřeby poskytovatele cloudu. - V případě privátního cloudu si lze někdy dodávání logů ze SIEMu přikoupit. Dodání vlastního SIEMu by bylo ekonomicky velmi náročné. - Sledování nesprávných aktivit zaměstnanců při zpracování dat přes DLP nelze, pokud si DLP sami nedodáte a nebudete jej spravovat. Cloudy DLP standardně neobsahují.	- V případě privátního cloudu a v některých případech i u veřejného cloudu si lze dodávání korelovaných sestav ze SIEMu sjednat. - Nedostanete však pod kontrolu celý SIEM, nebude tedy možné si vytvářet vlastní pohledy nebo sestavy podle aktuální potřeby.
---	---

Síla hesel a šifer

- V případě veřejného cloudu je plně pod kontrolou poskytovatele. - V případě privátního cloudu lze sjednat smluvně. - U používání fyzického nebo virtuálního serveru pro více firem vzniká často problém, že se protokoly, certifikáty a šifry neaktualizují s odvoláním na to, že hostované aplikace jiných firem by upgrade na poslední bezpečnostní standardy nesnesly.	- V případě veřejného cloudu se doporučuje ověřit sílu hesel a šifer zkusmo ještě před jeho sjednáním (přihlášením, kontrolou vlastního uloženého souboru). - V případě privátního cloudu je dobré si sjednat co nejsilnější přihlašovací údaje a použité šifry a občas ověřovat, jestli nasazené protokoly, certifikáty a šifry již nezastaraly a nemají bezpečnostní zranitelnost.
---	---

Zálohování a výpadky

- Na základě nařízení GDPR je správce odpovědný nejen za zabezpečení osobních údajů, ale i za jejich dostupnost a integritu. - Je tedy nezbytné provádět zálohování dat v cloudu. V případě problémů tak přejde poskytovatel na záložní servery nebo linky ve velmi krátké době. - Nikdy není možné s jistotou předem ověřit, zda poskytovatel skutečně data bezpečně zálohuje a jak by postupoval v případě katastrofického výpadku (např. požár).	- Dostupnost a integritu dat lze většinou ošetřit smluvně. (sankce při nesplnění by měly zpracovatele donutit, aby si zálohování, záložní servery a spojení zajistil). - V případě privátního cloudu je možné objednat např. další server jen pro účely zálohování a sjednat zaslání logů o průběhu zálohování. - Další možností pro případ výpadku cloudu je mít data uložena ještě jinde (např. v jiném cloudu, v podnikové síti atd.). Jedná se však o nákladné řešení a výhody využití cloudu se pak jeví jako sporné.
---	--

Veřejný cloud

Cloud kromě výhod přináší i řadu komplikací, a to obzvlášť při zpracování osobních údajů.

Dané komplikace jsou především právního charakteru, vznikají z technických vlastností cloudu a problémů spojených s bezpečným zpracováním dat. Veřejný cloud je tedy natolik problematický, že se jeho využití pro ochranu osobních údajů nedá doporučit.

To však neznamená, že například organizace nebudou platit pro své zaměstnance úložiště pro mobilní zařízení. V takovém případě by na těchto úložištích nesměli zaměstnanci uchovávat osobní údaje jiných osob.

Privátní cloud

Privátní cloud naopak většinou umožňuje doladit vzájemné vztahy a zabezpečení dat do takové míry, že jím lze zpracování dat v podnikové síti nahradit. Problémy cloudu, jako je trvající odpovědnost správce za únik dat, problém s fyzickou bezpečností server v cloudu atd., sice nadále přetrvávají, ale vyvažují je výhody cloudu, a to zejména vysoká dostupnost odkudkoliv. Provoz privátního cloudu je však značně náročnější než provoz veřejného cloudu, a to hlavně v oblasti zabezpečení.

Každá organizace si musí sama rozhodnout o nasazení cloudu v jednotlivých případech, a to na základě své analýzy rizik, funkčnosti a nákladů.

NA ZÁVĚR

Pevně věříme, že jste si našli čas na náš pravidelný magazín a že námi poskytnuté informace, jsou pro Vás užitečné a praktické.

Za celý kolektiv pracovníků firmy Vám přeji hezký den a hodně sil do následujících měsíců



Tomáš Urban
ředitel společnosti



Softbit Software, s.r.o.

Nad Dubinkou 1634

516 01 Rychnov nad Kněžnou

Tel.: 494 532 202, 494 534 354, fax: 494 377 63

e-mail: softbit@softbit.cz

www.softbit.cz



Tým společnosti Softbit Software s.r.o

Tomáš URBAN

- ✓ ředitel společnosti
- ✓ programátor účetnictví
- ✓ metodický konzultant informačních systémů



Simona URBANOVÁ

- ✓ ekonomka
- ✓ metodická konzultantka informačních systémů



Ing. Jeroným HOLÝ

- ✓ programátor majetek, výroba, jídelna
- ✓ metodický konzultant informačních systémů



Ing. Radim HOLÝ

- ✓ programátor sklady, prodej, odbyt
- ✓ metodický konzultant informačních systémů



Bc. Dana PEREMSKÁ

- ✓ administrativní pracovnice
- ✓ péče o zákazníky



David SMEJKAL

- ✓ hardware
- ✓ konzultant Vema HR, mzdy
- ✓ metodický konzultant informačních systémů



Tomáš HOLÝ

- ✓ programátor
- ✓ konzultant



Bc. Radek BERÁNEK

- ✓ všeobecný programátor
- ✓ konzultant Vema HR
- ✓ metodický konzultant informačních systémů



David URBAN

- ✓ všeobecný programátor

