Magazín GDPR

číslo 1/2020

SOFT bit software

… 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.

Také bychom Vás rádi seznámili s opatřeními, vyplývajícími z nařízení vlády ze dne 15. 3. 2020, ohledně vyhlášení celorepublikové karantény. V této době jsou naše IT služby prováděny pouze formou vzdáleného připojení, kromě případů, jako je odstranění havarijního stavu atd.

Rovněž naši pracovníci, pokud to není neodkladně nutné, pracují z domova. Z tohoto důvodu budeme rádi, když budete se svými požadavky kontaktovat přímo naše pracovníky na tel. číslech, která máme uvedena na webových stránkách zde.

Můžete rovněž využít telefonní linku naší centrály 494 532 202 nebo 494 534 354, která je k dispozici v pracovní dny od 8 do 16 hodin.

Děkujeme za pochopení.

Přejeme Vám příjemné čtení

Ing. Dana Peremská
pracovník zákaznické podpory

Obsah magazínu

Jaká jsou Vaše práva a povinnosti při kontrole z ÚOOÚ

Povinnosti správce v případě kontaktování ÚOOÚ z důvodu šetření stížnosti subjektu údajů nebo jiného podnětu, nejsou v GDPR konkrétně upraveny. Je zde však **obecná povinnost** všech správců a zpracovatelů, a to spolupráce s dozorovým úřadem při plnění jeho úkolů.

Co může požadovat dozorový úřad

Dozorový úřad může správci či zpracovateli nařídit, aby poskytl veškeré informace, které jsou potřebné k plnění jeho úkolů. Může požadovat přístup ke všem osobním údajům a ke všem informacím, jenž potřebuje k výkonu svých úkolů, stejně tak i přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu ke všem zařízením a prostředkům určeným ke zpracování osobních údajů, a to v souladu s procesním právem EU nebo členského státu.

Co může snížit riziko stížnosti

Je dobré, aby **veškerá komunikace se subjekty údajů a správci či zpracovateli probíhala korektně a včas.** Aby potřebná dokumentace a prostředky zpracování splňovaly stanovené požadavky. Všichni zaměstnanci správce či zpracovatele by měli být proškoleni o otázkách řádného zpracování a zabezpečení osobních údajů. Toto vše může vést k minimalizaci rizika stížností ze strany subjektů údajů a následného postupu ÚOOÚ.

ÚOOÚ se zabývá stížnostmi subjektů údajů, dále i jinými podněty, které obdrží od dozorových úřadů jiných členských států EU, soud, policie, na základě upozornění ve sdělovacích prostředcích atd. **Každý podnět je ÚOOÚ povinen prověřit a prošetřit**, ne však pokaždé je nutné provést kontrolu u daného subjektu.

Úkony před zahájením kontroly

Správci či zpracovatelé by měli při jakémkoli kontaktu ze strany ÚOOÚ **reagovat rychle a s odbornou znalostí**, můžete se tak vyhnout kontrolám a případným postihům.

Před zahájením kontroly ÚOOÚ provede opatření podkladů pro posouzení, zda zahájit kontrolu. Pokud kontrolovaná osoba není ochotna dobrovolně spolupracovat, může to být signál k zahájení kontroly. Pokud naopak ÚOOÚ při předběžném šetření nezjistí důvod pro zahájení kontroly, ustoupí od jejího provedení. **Předběžné šetření ÚOOÚ může probíhat jakoukoli formou, např. telefonicky, e-mailem.** U správce či zpracovatel, který jmenoval pověřence pro ochranu osobních údajů, **ÚOOÚ bude komunikovat právě s tímto pověřencem.** Kontaktní údaje na pověřence, musí správce či zpracovat oznámit po jeho jmenování ÚOOÚ.

Zahájení kontroly ÚOOÚ

ÚOOÚ zahájí kontrolu v případě, že bude mít pochybnosti o souladu zjištěného stavu se stavem požadovaným. V rámci kontroly jsou identifikovány konkrétní nedostatky. Rozhodnutí ÚOOÚ zahájit kontrolu je výhradně z úřední povinnosti, neexistuje právní nárok stěžovatele na zahájení kontroly. Povinností ÚOOÚ je však informovat stěžovatele o vývoji a výsledku šetření jeho stížnosti.

O zahájení kontroly musí být kontrolovaný informován písemně nebo ústně kontrolující osobou na místě kontroly. Kontrolující osoba se prokáže průkazem. V případě, že je kontrola zahájena bez přítomnosti kontrolované osoby nebo jejího zástupce, musí být kontrolovaná osoba o zahájení kontroly dodatečně informována kontrolující osobou. Všichni zaměstnanci potenciální kontrolované osoby by měli být **připraveni a poučeni, jak postupovat v případě kontroly ÚOOÚ** (především znalost povinností v průběhu kontroly).

Jak postupovat v případě zahájení kontroly ÚOOÚ

- ✓ při písemném oznámení kontroly *zajistit přítomnost oprávněné osoby* v místě kontroly (např. statutární orgán nebo osoba pověřená k právním jednáním se státními úřady) nebo požádat o nový termín kontroly
- ✓ *poučit zaměstnance* o jejich povinnosti prokázat kontrolující osobě svou totožnost a poskytnout jí součinnost při výkonu kontroly
- ✓ *připravit pro kontrolu základní dokumentaci*
  - ➥ záznamy o činnostech zpracování
  - ➥ texty souhlasů subjektů údajů
  - ➥ důkazy o splnění informační povinnosti
  - ➥ směrnici o zpracování osobních údajů
  - ➥ dokumentaci o přijatých opatřeních k zabezpečení osobních údajů
  - ➥ evidence vedené podle GDPR (evidence stížností a žádostí, evidence bezpečnostních incidentů, evidence souhlasů a odvolaných souhlasů, smlouvy o zpracování osobních údajů atd.)
- ✓ *zkontrolovat veškeré prostředky a prostory zpracování* (IT systémy, kamerové systémy, kartotéky, pracovní stoly, apod.), případně provést rychlý interní audit
- ✓ *vyžadovat od kontrolující osoby předložení průkazu* a dalšího dokladu k prokázání její totožnosti
- ✓ *namítnout případnou podjatost* kontrolující osoby
- ✓ *umožnit kontrolující osobě vstup do všech prostor* a využívání technických prostředků nezbytných pro výkon kontroly
- ✓ *poskytnout kontrolující osobě veškeré požadované podklady* a případně též originální dokumenty
- ✓ *vyžadovat od kontrolující osoby potvrzení o zajištěných originálních podkladech* a následně jejich vrácení
- ✓ *poskytnout kontrolující osobě další součinnost*
- ✓ *upozornit kontrolující osobu, případně ÚOOÚ, pokud by kontrola probíhala způsobem, který nepřiměřeně zasahuje do práv a oprávněných zájmů kontrolované osoby*
- ✓ *seznámit se s obsahem protokolu o kontrole a podat včas případné námitky*
- ✓ *provést neprodleně nápravu* případných zjištěných nedostatků a připravit o tom zprávu pro ÚOOÚ
- ✓ v případě rozhodnutí o uložení pokuty podat včas rozklad proti tomuto rozhodnutí, pokud je to důvodné
- ✓ při zamítnutí rozkladu podat včas žalobu na ÚOOÚ k příslušnému krajskému soudu, pokud je to důvodné

Jsou Češi připraveni na kyberútoky

Ve střední Evropě se stanou každoročně obětí hackerských útoků dvě ze tří firem či organizací. V rámci států Evropské unie se **Česko nachází v dolní třetině žebříčku připravenosti** vůči kybernetickým útokům a jejich prevenci po technické i personální stránce. Útoky jsou na internetu hůře rozpoznatelné, a to svou sofistikovaností a zároveň snazší proveditelností. Společnosti se v současné době spoléhají především na bezpečnostní technologie, což však není dostačující.

Bezpečnostní opatření

Základním bezpečnostním opatřením je definování přesných rolí a přesné určení reakčního plánu na odstranění kybernetického útoku či incidentu. Je důležité analyzovat, jak se kybernetické útoky změní a jak se bude transformovat následné riziko.

Ukládání údajů o společnostech do veřejného cloudu považuje většina IT pracovníků za relativně bezpečné. Nejvyšší zabezpečení však poskytují šifrované cloudové úložiště, jenž jsou v souladu s GDPR.

Riziko zneužití údajů

Velké riziko zneužití údajů naopak představují externí přenosná paměťová a disková média, a to USB klíče, disky, ale i notebooky.

Biometrické údaje

Nejčastější obranou proti vznikajícím hrozbám jsou v současnosti biometrické údaje. Jedná se o údaje, které jsou pro každého jedince unikátní a jednoznačně jej identifikují, např. snímek obličeje, otisk prstu, snímek oční duhovky, snímek sítnice, podpis, hlas.

Využití biometrických údajů v souladu s GDPR je značně problematické. Lze očekávat, že se kyberzločinci v budoucnosti zaměří právě na biometrické údaje, neboť se tyto údaje budou muset uchovávat globálně. Kyberzločinci se tak nebudou omezovat na krádež pouze čísla kreditní karty oběti, ale na krádež otisku prstů, identifikaci hlasu a skenování sítnice.

Nová generace 5G sítě

Jednou z nejnáročnějších výzev v oblasti kybernetické bezpečnosti bude nová generace 5G sítě. Tyto nové sítě přinesou spoustu výhod, a to nejen rychlejší internet. Poskytne architekturu na propojení nových průmyslových odvětví, geografických oblastí a komunit. Nebude se však jednat pouze o výhody, zároveň **dojde k výraznému rozšíření počítačové kriminality v reálném světě** s důsledky, které ještě nejsou známy. Útočník bude mít okamžitý přístup k sítím a je pouze na správcích sítí, do jaké míry budou zranitelné. Infrastruktura inteligentních míst bude obsahovat systémy propojené v nové, nevídané míře, což bude kritické pro fungování života ve městech. Vyřazení infrastruktury by způsobilo velké problémy a škody, což představuje velkou motivaci pro tvůrce ransomwaru. Na účinná opatření bude velmi málo času, příkladem může být rozšíření útoku WannaCry v roce 2017, které trvalo několik dní. V 5G síti by mohl tento útok být rozšířen během několika sekund.

V případě, že se stanete obětí kybernetického útoku, je nutné tuto skutečnost ohlásit prostřednictvím formuláře Ohlášení porušení zabezpečení osobních údajů dle GDPR, vzor ohlášení zde.

Bezpečnost na internetu – nejdůležitější pojmy

Bluetooth – bezdrátový komunikační standard, který je určen k propojení zařízení, jako jsou mobilní telefony, notebooky a kapesní počítače. Při nezabezpečení zařízení, které je vybaveno bluetooth hrozí nebezpečí krádeže dat.

Bluetoothing – netradiční způsob seznámení s pomocí zařízení vybaveného bluetooth. Tuto funkci aktivujete, pokud je ve Vašem dosahu někdo jiný s aktivovanou funkcí bluetooth, tak se název jeho zařízení či konkrétní přezdívka objeví na displeji. Pak už stačí pouze odeslat prostřednictvím bluetooth svoji vizitku a čekáte, zda ten „někdo“ odpoví.

Bullying (týrání) – šikanování a ponižování jednotlivců nebo skupin formou osobních útoků vedených prostřednictvím kanálů elektronické komunikace, např. e-mail, instant messaging nebo textové zprávy (SMS).

Cookies (koláčky) – malé kousky informací, uchovávané v jednoduchých textových souborech, umístěných na Váš počítač u webové sítě. Cookies mohou být čteny webovými stránkami během Vašich pozdějších návštěv. Informace uložená v cookie může mít vztah k Vašemu chování při procházení webové stránky, nebo obsahovat jedinečné identifikační číslo, pomocí kterého si Vás bude webová stránka pamatovat při Vaší příští návštěvě. Existují dva druhy cookies, trvalé a relační. *Trvalé cookies* jsou uloženy na Vašem pevném disku po mnoho měsíců nebo let. *Relační cookies* jsou uloženy ve vyrovnávací paměti během Vaší návštěvy webové stránky a jsou automaticky smazány z Vašeho počítače v okamžiku, kdy se odpojíte od internetu.

Cyber stalking (kybernetický lov) – zneužívání on-line komunikace k obtěžování a zastrašování vybraných uživatelů. Oběti tohoto typu chování jsou pronásledovány a obtěžovány spamem, zanecháváním nepřístojných vzkazů v návštěvních knihách, na chatu, zasíláním virů, atd.

Flaming – umísťování vědomě nepřátelských a urážlivých vzkazů na internet s cílem někoho rozhněvat a urazit.

IP adresa – identifikační detaily pro Váš počítač (nebo Vašeho poskytovatele internetového připojení), vyjádřené v kódu „internetového protokolu). Každý počítač připojený k internetu má jedinečnou IP adresu, ačkoliv adresa nemusí být stejná při každém připojení se k internetu.

Pharming – jedna z variant krádeže osobních údajů, které jsou získávány po infikování počítače zákeřným programem. Uživateli je pak místo např. požadované oficiální stránky banky podstrčena falešná stránka, která sbírá přístupové údaje a osobní data k jejich dalšímu zneužití.

Phishing – krádež citlivých informací, např. údajů o platební kartě či krádež jména a hesla k nějaké službě. Nejčastějším příkladem je falešný e-mail, tvářící se jako odeslaný z Vaší banky, v němž je požadavek o ověření totožnosti. Po kliknutí na odkaz je uživatel zaveden na falešnou stránku (která se však tváří, že je v pořádku), kde odevzdá své údaje a následně přijde o peníze.

Spam – obecný výraz pro hromadně rozesílanou, nevyžádanou elektronickou poštu. Nevyžádaná komunikace není výjimečná pouze pro internet, většina z nás pravidelně dostává nechtěnou poštu nebo je bez předchozího vyžádání kontaktována telefonicky.

Spoofing – technika, při které určitý počítač v rámci sítě internet předkládá falešnou IP adresu a vydává se tak za někoho jiného. Cílem je získat přístup k informacím, které by jinak uživatel získat nemohl (např. placené webové stránky), nebo zabránit své vlastní identifikaci. S využitím této techniky lze také nelegálně vstoupit do cizího počítače.

Spyware – ilegální software, který se do počítače nainstaluje automaticky, obvykle skrze bezpečnostní slabinu systému. Tam monitoruje aktivitu uživatele a odesílá informace svému autorovi. Získaná data jsou využívána k lepšímu cílení reklamy na uživatele, ale také k odposlechu hesel.

Zdroj: Úřad pro ochranu osobních údajů

Novela informačního zákona – dopad na školy

Účinnost od 1. 1. 2020

Novela zákona o svobodném přístupu k informacím nabyla účinnosti 1. 1. 2020. Tato novela mění pojetí přístupu k poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Podle zákonodárců novela zrychlí a zjednoduší řešení sporů souvisejících s poskytováním informací.

Hlavními změnami jsou zavedení tzv. informačního příkazu, přezkumného řízení, ochrany proti nečinnosti a rozšíření působnosti ÚOOÚ s dohledem nad právem na informace. Principy poskytování informací dle zákona č. 106/1999 Sb., se však nemění.

Nejčastějšími žádostmi o poskytnutí informací jsou informace o platech zaměstnanců, informace o výdajích školských zařízeních a informace o detailech některých smluv. Detaily smluv jsou např. dodavatel potravin pro školní jídelnu, výše odměny pověřence pro ochranu osobních údajů, výše odměny správce IT atd.

Jak se vypořádat se žádostmi o poskytnutí informací, které nechcete sdělovat?

Zaměstnavatel může odmítnout žádost o poskytnutí informací o platu zaměstnance, jestliže nejsou splněny všechny následující podmínky:

- účelem vyžádání informací je přispět k diskusi o věcech veřejného zájmu,
- samotná informace se týká veřejného zájmu,
- žadatel o informace plní úkoly nebo poslání dozoru veřejnosti,
- informace existují a jsou dostupné.

Kdy a jak musíte žádosti o poskytnutí informací vyhovět?

Vždy musíte poskytnutí informací posuzovat i z pohledu ostatních právních norem, především předpisů o ochraně osobních údajů. Ze žádosti o poskytnutí informací musí být jasné, kdo je žadatelem a jaké informace požaduje. Pokud jsou tyto informace nejasné, vyzve škola žadatele k doplnění žádosti, a to do 7 dnů od obdržení žádosti. V případě, že žádost obsahuje všechny potřebné údaje, **škola musí žádosti vyhovět do 30 dnů** ode dne obdržení žádosti, nebo má povinnost sdělit důvody neposkytnutí informací.

V některých případech je nejjednodušší žádosti o poskytnutí informací vyhovět, vyhnete se tak vleklým sporům. Vyhovění žádosti však nesmí být školou nepřiměřeně zpoplatněno. Škola může pouze požadovat úhradu reálně vynaložených administrativních nákladů za poskytnutí informací. Jestliže však žadatel požaduje informace, na které opravdu nemá nárok, odmítnutí žádosti nebude představovat pro školu žádné riziko.

Nové možnosti pro neúspěšné žadatele

Nově spadá agenda řešení sporů souvisejících s neposkytnutím informací do kompetencí ÚOOÚ. **ÚOOÚ má tedy úřední povinnost zahajovat přezkumné řízení.** Přezkumné řízení bude zahájeno, pouze pokud bude možné důvodně pochybovat, že rozhodnutí o neposkytnutí informací je v souladu s právními předpisy. V případě, že ÚOOÚ shledá, že neexistují podmínky pro zahájení přezkumného řízení, sdělí tuto skutečnost, s uvedením důvodů a ve lhůtě 30 dnů, žadateli o poskytnutí informací. Jestliže však ÚOOÚ shledá, že bylo **odmítnutí žádosti o poskytnutí informací neoprávněné, postupuje dále k tzv.**

informačnímu příkazu. Jedná se o příkaz poskytnout informace. I proti informačnímu příkazu se můžete bránit, pokud jej budete považovat za nezákonný.

Často kladené otázky

Lze uchovávat v osobním spise zaměstnance kopie vysvědčení a certifikátů absolvovaných školení, které souvisejí s pracovním popisem práce zaměstnance během jeho platného pracovního poměru?

Právním důvodem pro uchovávání daných dokumentů je oprávněná zájem zaměstnavatele nebo u některých pracovních pozic splnění právní povinnosti. Při uchovávání musí být vždy dodrženy základní zásady GDPR. Jakmile pracovní poměr skončí, nebude nadále žádný důvod pro další uchovávání těchto dokumentů.

Je nutné, aby na souhlasu se zpracováním osobních údajů žáků byl souhlas a podpis obou zákonných zástupců žáka?

Zákon stanovuje, že rodiče vykonávají rodičovskou odpovědnost ve vzájemné shodě. Tato odpovědnost však nemá blíže specifikovanou formu. Lze tedy konstatovat, že v případě platnosti souhlasu se zpracováváním osobních údajů žáka postačí podpis jednoho zákonného zástupce (rodiče nebo poručníka), jestliže dané jednání nerozporuje druhý rodič.

Matka či otec poskytli přihlašovací údaje k elektronické žákovské knížce další osobě (např. babičce). Lze danou situaci řešit prostřednictvím GDPR?

Nikoli. Jedná se o záležitost rodiny, jakým způsobem si nastaví možnosti kontroly prospěchů dítěte mezi sebou a to jak u klasických žákovských knížek, tak i prostřednictvím vzdáleného přístupu k údajům v elektronické žákovské knížce. Pravidla ochrany osobních údajů nijak nezasahují do potřebného sídlení přístupu do elektronické žákovské knížky, zejména mezi rodinnými příslušníky, kteří se podílejí na výchově dítěte.

Potřebují e-shopy ke zpracování osobních údajů souhlas zákazníků?

K běžnému provozu internetového obchodu není nutné obstarávat souhlas se zpracováním osobních údajů, jelikož se jedná o zpracování údajů v rámci smluvní agendy (vyřizování objednávek a nákupů zákazníků, následné plnění zákonem stanovené povinnosti evidence dokladů, atd.).

Jak mění GDPR zvláštní pravidla pro zacházení s cookies a pro marketing?

V těchto oblastech GDPR zásadním způsobem nic nemění ani více samostatně neupravuje. Dosavadní pravidla pro používání cookies a zpracování osobních údajů za účelem elektronické reklamy nebyla ani dosud upravena zákonem o ochraně osobních údajů, nýbrž zvláštními předpisy v gesci Ministerstva průmyslu a obchodu (zákon č. 127/2005 Sb. a č. 480/2004 Sb.), a budou podstatně novelizována až přijetím dalšího předpisu EU, tzv. nařízení o ePrivacy.

Zdroj: Úřad pro ochranu osobních údajů

Nabídka základních služeb GDPR

Naší prioritou je dodávat našim zákazníkům kompletní služby. Z tohoto důvodu 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.

Rádi Vám umíme nabídnout:

- ✓ Zpracování úvodního vnitřního auditu k evidenci, uchovávání a zabezpečení veškerých informací o fyzických osobách, a to jak v elektronické, tak i v listinné podobě.
- ✓ Na základě tohoto auditu je zpracována vnitropodniková směrnice k nakládání s osobními údaji podle nařízení GDPR, která popisuje jednotlivé části v informačních systémech a evidenci dokumentů ve Vaší společnosti a navrhujeme taková řešení, která povedou k zajištění vyšší bezpečnosti dat o fyzických osobách.
- ✓ Toto by měl být začátek naší spolupráce. Doporučujeme revizi vnitropodnikové směrnice vždy za určité období (ideální rok), kdy se provedou inventarizace změn proti předchozímu období a vyhodnotí se provedené změny.
- ✓ Školení všech pracovníků společnosti, kteří přicházejí do styku s osobními údaji subjektu údajů.
- ✓ S každým klientem k tomuto uzavíráme smlouvu pro služby „Pověřence pro ochranu osobních údajů“, kde Vám garantujeme zajištění komplexního servisu pro služby k GDPR včetně metodické podpory. Tato služba je standardně bez žádného paušálního poplatku.
- ✓ V případě, že by ve Vaší společnosti došlo k incidentu se ztrátou osobních dat a byli jste za tuto chybu vyšetřováni, nabízíme i spolupráci při řešení těchto situací. Nejsme však právníci tak, abychom Vás zastupovali u případného soudu. Věřím, že s naší pomocí se těmto událostem však vyhnete.

Ceník základních služeb GDPR	
GDPR – vnitropodniková směrnice	**7.000,- Kč**
Práce spojené s lokalizací směrnice na podmínky Vaší společnosti	**900,- Kč/hod**
Školení pracovníků	**1.200,- Kč/hod**
Cestovní výdaje při osobních návštěvách	**9,- Kč/Km + 450,- Kč/hod strávený čas na cestě**
Konzultace pověřence pro ochranu osobních dat pana Tomáše Urbana	**900,- Kč/hod**

Ceny jsou uvedeny bez DPH 21 %.

Certifikovaný pověřenec pro ochranu osobních dat:
TOMÁŠ URBAN
e-mail: tomas.urban@softbit.cz
tel.: 603 449 244

Nabídka služeb GDPR – pro naše zákazníky

V minulých letech 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 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.

Ceník služeb GDPR	
Aktualizace směrnice GDPR pro rok 2020	**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 %.

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.

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
(tel. 603 449 244)
- ✓ ředitel společnosti
- ✓ programátor účetnictví
- ✓ metodický konzultant informačních systémů

Simona URBANOVÁ
(tel. 736 753 733)
- ✓ ekonomka
- ✓ metodická konzultantka informačních systémů

Ing. Jeronym HOLÝ
(tel. 736 159 010)
- ✓ programátor majetek, výroba, jídelna
- ✓ metodický konzultant informačních systémů

Ing. Radim HOLÝ
(tel. 604 632 774)
- ✓ programátor sklady, prodej, odbyt
- ✓ metodický konzultant informačních systémů

Ing. Dana PEREMSKÁ
(tel. 736 753 735)
- ✓ administrativní pracovnice
- ✓ péče o zákazníky

David SMEJKAL
(tel. 603 365 779)
- ✓ hardware
- ✓ konzultant Vema HR, mzdy
- ✓ metodický konzultant informačních systémů

Tomáš HOLÝ
- ✓ programátor
- ✓ konzultant

Bc. Radek BERÁNEK
(tel. 736 753 734)
- ✓ všeobecný programátor
- ✓ konzultant Vema HR
- ✓ metodický konzultant informačních systémů

David URBAN
- ✓ všeobecný programátor