Magazín GDPR

číslo 3/2020

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.

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

Ing. Dana Peremská
pracovník zákaznické podpory

Obsah magazínu

Analýza rizik – základní požadavek GDPR

Analýza rizik je nezbytná pro správné zpracování osobních údajů. Z této analýzy by měla vycházet všechna další opatření týkající se zpracování osobních údajů. Při zpracování analýzy je důležité brát rizika z pohledu subjektu údajů a ne z pohledu správce údajů.

Aktivum (asset)

Hodnota, kterou chceme chránit před hrozbami (majetek, zařízení, obraz, software, auta, počítače, strojní vybavení, data a osobní údaje,…).

Hrozba (threat)

Negativní události, osoby či aktivity, které mají zájem či potenciál poškodit aktivum (hodnotu), hrozba má nežádoucí vliv na bezpečnost nebo může způsobit škodu, ztrátu, či nežádoucí změnu. Hrozba způsobuje škody, které lze vyčíslit jako ztrátu, tzn. náklady na znovuobnovení aktiv nebo náklady na odstranění následků škod. Důležité je rozeznat úroveň nebezpečnosti hrozby.

- ✓ **živelné pohromy** – povodeň, požár, kalamita
- ✓ **havárie** – dopravní nehoda, kontaminace vody, výbuch, radiace
- ✓ **společenské jevy** – válečný konflikt, zločin
- ✓ **ekonomické jevy** – finanční krize, pohyb měnového kurzu, nedostupnost úvěru
- ✓ **chování jednotlivců** – chyba obsluhy, krádež, neoprávněné užívání či zneužití pravomoci

Zranitelnost (vulnerability)

Označení slabiny či nedostatku aktiva, který umožňuje uplatnění hrozby.

Riziko (risk)

Potencionální problém, nebezpečí vzniku škody, možnost selhání nebo neúspěchu, poškození, ztráty či zničení. Pravděpodobnost, že hrozba naruší důvěrnost, integritu nebo dostupnost.

Důvěrnost, integrita, dostupnost (confidentality, integrity, availability)

- ✓ **integrita** – zajištění správnosti a úplnosti informací
- ✓ **narušení integrity** – nežádoucí změna dat nebo osobních údajů
- ✓ **důvěrnost** – informace a osobní údaje jsou přístupné nebo sděleny pouze oprávněným osobám
- ✓ **narušení důvěrnosti** – nežádoucí zpřístupnění určitých informací, dat nebo osobních údajů
- ✓ **dostupnost** – přístupnost informací, dat a osobních údajů pro oprávněné uživatele v případě potřeb

Opatření (countermeasure)

Opatření, která jsme udělali pro snížení zranitelnosti. Fyzická, logická a administrativní bezpečnost.

Poskytoval cloudu je zpracovatelem – ano či ne?

Zpracovatel Zpracování

Zpracovatel je taková osoba, která zpracovává osobní údaje pro správce.

Zpracování je jakákoli operace nebo soubor operací s osobními údaji či se soubory osobních údajů, která je prováděna pomocí či bez pomoci automatizovaných postupů, jako je mimo jiné i uložení.

Zásada integrity a důvěrnosti

Dále existuje zásada integrity a důvěrnosti, dle které správci i zpracovateli musí zpracovávat osobní údaje způsobem, jenž zajistí náležité zabezpečení osobních údajů včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením či poškozením.

Zpracování údajů zpracovatelem

Důvod 81 Obecného nařízení EU o ochraně osobních údajů stanovuje: *„Provádění zpracování zpracovatelem by se mělo řídit smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které by zavazovaly zpracovatele vůči správci a v nichž by byl stanoven předmět a doba trvání zpracování, povaha a účely zpracování, typ osobních údajů a kategorie subjektů údajů, s přihlédnutím ke konkrétním úkolům a povinnosti zpracovatele v souvislosti se zpracováním, jež má být provedeno, a riziko pro práva a svobody subjektů údajů.“*

Kdy se stává zpracovatel zpracovatelem

Zpracovatel se stává zpracovatelem v momentě, kdy začne z pokynu správce zpracovávat osobní údaje. Zda má zpracovatel přístup k osobním údajům či nikoli, nehraje žádnou roli. Samo uložení a uchovávání je operací zpracování. Dle výše zmíněných definic je tedy patrné, že **poskytovatel cloudu je zpracovatelem.**

GDPR chrání subjekty údajů nejen před možným zneužitím osobních údajů, ale i před jejich ztrátou nebo znehodnocením. Další povinností dle GDPR je schopnost obnovit dostupnost osobních údajů. Tuto povinnost lze definovat jako povinnost provádět zálohy. Poskytovatel cloudu má z povahy věci kontrolu nad daty a pokud by například „vypnul“ servery, došlo by ke ztrátě dat.

Vyjádření WP29

WP29 (Pracovní skupina pro ochranu údajů zřízená podle článku 29) vydala přímo ke cloud computingu toto vyjádření: *„Pokud poskytovatel cloudových služeb zajišťuje prostředky a platformy a jedná jménem zákazníka cloudových služeb, pak se považuje za zpracovatele údajů.“*

Biometrická identifikace a autentizace – mýty a omyly

Podle zprávy vypracované evropským inspektorem ochrany údajů a španělským Úřadem pro ochranu osobních údajů Vám přinášíme 14 nejčastějších mýtů a omylů souvisejících s biometrickou identifikací a autentizací.

Identifikace

Identifikace je postup porovnání dat jednotlivce, aby byl identifikován ve vztahu k údajům každého jednotlivce v rámci této skupiny.

Autentizace

Autentizace je ověření identity subjektu (osoby, systému). Porovnává pouze údaje daného subjektu s údaji tvrzené identity.

Způsoby autentizace:

- co subjekt má – identifikační karta, dokument, platební karta, atd.
- co subjekt zná – heslo, PIN, atd.
- čím subjekt je – biometrické údaje

Biometrické údaje

Jedná se o údaje, které jsou pro každého jedince unikátní a jednoznačně jej identifikují. Například snímek obličeje, otisk prstu, snímek oční duhovky, snímek sítnice, podpis, hlas.

14 mýtů a omylů:

1. „Biometrická informace je uchovávána v samotném algoritmu.“

Algoritmus je metoda, přednastavená sada operací nebo návod, nikoli však prostředek pro uchovávání biometrických údajů. **Shromážděné biometrické informace jsou zpracovávány dle standardně definovaných postupů a výsledek tohoto postupu je uložen v datových záznamech, tzv. podpisech, vzorcích nebo šablonách.** Tyto vzorce číselně zaznamenávají fyzické vlastnosti, čímž umožňují rozlišit jednotlivé osoby. Existují však techniky strojového učení, které předávají části svých tréninkových datových sad modelům, které vytvářejí. Některé z těchto technik jsou užívané při biometrické identifikaci a autentizaci.

2. „Užívání biometrických údajů je stejně rušivé jako jakýkoliv jiný identifikační/autentizační systém.“

Shromážděné biometrické údaje odhalují o subjektu v průběhu procesu autentizace a identifikace více informací než hesla nebo certifikáty. O subjektu mohou být odhaleny údaje jako rasa, pohlaví, duševní stav, nemoci, genetické vlastnosti, fyzické vady, užívání látek atd.

3. „Biometrická identifikace/autentizace je přesná.“

Biometrická identifikace/autentizace je založena na pravděpodobnosti, není tedy přesná jako heslo nebo certifikáty. Příkladem je otisk prstu, který je z 96% podobný jednomu z X. Existuje určitá míra chybné shody a chybné neshody, která závisí na snímacím zařízení a podmínkách, za kterých se sejmutí uskutečnilo (světlo, čistota senzoru,…). Přesnost některých biometrických údajů (např. otisk prstů) závisí na věku osoby a je ovlivněna jejím stárnutím.

4. „Biometrická identifikace/autentizace je natolik přesná, aby vždy rozlišila mezi dvěma osobami.“

Biometrická podobnost mezi sourozenci nebo příbuznými je pro biometrické systémy matoucí. Také podmínky v nekontrolovaných prostředcích (rozpoznávání obličeje na veřejném prostranství, užívání obličejových nebo antivirových masek) vedou ke zvýšené chybovosti a záměna je tedy pravděpodobnější.

5. „Biometrická identifikace/autentizace je vhodná pro všechny osoby.“

Někteří lidé nemohou užívat určitý typ biometricky, jelikož systém nerozpozná jejich fyzické vlastnosti. Jedná se o případy zranění, nehod, zdravotního stavu (např. ochrnutí) atd. Některé nekompatibility mohou být dočasné jiné trvalé. Trvalá biometrická nekompatibilita může být jedním z faktorů vedoucích až ke společenskému vyloučení.

6. „Postup biometrické identifikace/autentizace nelze obejít.“

Existují postupy a techniky, které umožňují obejít biometrické autentizační systémy a předstírat identitu jiné osoby. Příkladem je používání masek nebo kopírování otisků prstů, k čemuž není potřeba mít rozsáhle technické znalosti či ekonomické zdroje. Některé postupy a techniky jsou speciálně navrženy k přelstění obrazových rozpoznávacích systémů a mohou být užity k přelstění biometrické identifikace. Jedná se o tzv. „nepřátelské systémy“.

7. „Biometrická informace nemůže být prozrazena.“

Většina osobních biometrických vlastností není chráněna a může být zachycena na dálku (např. obličej, otisky prstů, směr pohybu, atd.).

8. „Jakékoliv biometrické zpracování předpokládá identifikaci/autentizaci.“

Není nezbytně nutné, aby biometrické zpracování obsahovalo identifikaci nebo autentizaci. Například zpracování biometrických údajů pohybu myši využívané k určení toho, zda k webové stránce přistupuje robot, využívá zacházení s biometrickou informací pro účely rozlišení člověka od stroje. Zpracování biometrických údajů může být také prováděno ke zjištění, zda se lidský nebo zvířecí narušitel pohybuje v určitém prostoru nebo v případě digitálních systémů rozlišujících muže, ženy a děti.

9. „Biometrické identifikační/autentizační systémy jsou pro uživatele bezpečnější.“

V každém systému, ve kterém jsou zpracovávány biometrické údaje, může dojít k porušení zabezpečení. Neoprávněný přístup k biometrickým údajům v systému by umožnil nebo ulehčil (v případě více autentizačních faktorů) přístup k dalším systémům užívajícím tytéž biometrické údaje. Následek by mohl být stejný jako v případě používání stejného hesla u různých odlišných systémů. Rozdílem je však, že jednou kompromitovaná biometrická informace nemůže být změněna nebo zrušena, jako v případě hesla.

10. „Biometrická autentizace je silná.“

Silný autentizační systém je takový, který vyžaduje poskytnutí alespoň dvou faktorů z toho, co znáte, máte nebo jste (biometrika). Autentizační proces používající pouze biometrické údaje je tedy dle této definice slabý. Biometrická autentizace často vyžaduje předchozí registraci nebo identifikaci, u které (např. rozpoznávání obličeje) je nutné porovnání s fotografií v dokladu totožnosti. **Pokud je ale po identifikačním postupu autentizační proces pouze biometrický, je systém slabý.**

11. „Biometrická identifikace/autentizace je uživatelsky přívětivější.“

Záleží na použité technologii, okolnostech, vnímání a kultuře každého uživatele. Kromě toho, že biometrická identifikace/autentizace není vhodná pro všechny osoby, mohou nastat i další problémy, které negativně ovlivní vnímání uživatele. Jedná se o pocit narušení soukromí, selhání biometrických systémů, které zabrání přístupu ke službám, neexistence nebo nevhodnost nebiometrických alternativ nebo potřeba provést registraci u každé entity.

12. „Biometrickou informaci převedenou do hashe nelze obnovit.“

Existují studie, které ukazují, že hash může být „návratný“, tzn. že je možné získat původní biometrický vzor, a to zvláště v případě, když je porušeno tajemství klíče užitého ke generování hashe.

13. „Uložená biometrická informace neumožňuje rekonstrukci původní biometrické informace, ze které byla získána.“

Uložená biometrická informace umožňuje částečnou rekonstrukci původního biometrického údaje (např. obličej). Částečná rekonstrukce biometrického údaje má často dostatečnou přesnost pro to, aby ji jiný biometrický systém rozpoznal jako původní údaj. Existují např. studie obličejové biometrické informace, které ukazují, že je možné získat věrohodné zobrazení z robotického portrétu (počítačem vytvořený portrét). Přesnost rekonstrukce závisí na množství shromážděných biometrických informací.

14. „Biometrická informace není interoperabilní.“

Systémy zpracovávající biometrické informace jsou vyvíjeny podle takových standardů, aby se zajistila jejich interoperabilita. Systémy, které porovnávají výsledek hashovací funkce aplikované na biometrické vzory, mohou být interoperabilní jednoduchou metodou, a to sdílením klíčů použitých při hashovacím procesu.

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	**od 1.900,- 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 magazín GDPR 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