Orbán Zoltán
Logipen Kft.
8174 Balatonkenese, Simon István u. 19.

Tárgy: szakértői vélemény
A www.webcafeteria.hu
oldalról

SZAKVÉLEMÉNY

Fülöp Tamás Miklós
igazságügyi informatikai szakértő
2230 Gyömrő, Rudolf u. 5.
Nyilvántartási szám: 8334

Fülöp Tamás Miklós
igazságügyi szakértő

Orbán Zoltán
Logipen Kft.
8174 Balatonkenese, Simon István u. 19.

Tárgy: szakértői vélemény
A www.webcafeteria.hu
oldalról

SZAKVÉLEMÉNY

A szakvéleményt a a www.webcafeteria.hu oldalt fejlesztő Logipen Kft. és Software & Art Kft. felkérésére készítettem. A szakvélemény a vizsgálat időpontjában fennálló állapotok alapján készült. A szakértői véleményt a vizsgálattal kapcsolatban az leírások és egyéb nyilvános és belső információk vizsgálata alapján, valamint a tárgyterület szakirodalmának és ajánlásainak figyelembevételével készítettem el. A vizsgálat eredményét esetlegesen befolyásoló új információk felmerülése vonatkozásában a szakvélemény változtatásának jogát fenntartom.

Ez a szakértői vélemény 12 db számozott oldalból áll.

Fülöp Tamás Miklós
igazságügyi informatikai szakértő
2230 Gyömrő, Rudolf u. 5.
Nyilvántartási szám: 8334

Fülöp Tamás Miklós
igazságügyi szakértő

1. Tartalomjegyzék

2. Feladat

A Logipen Kft. által üzemeltetett www.webcafeteria.hu oldal vizsgálata, különös tekintettel a biztonsági megoldásokra.

3. A vizsgálat módszere

A rendszer tervezése és fejlesztése során létrejött dokumentumok, a rendszer tesztelése, a vonatkozó jogszabályok áttekintése, a rendszer biztonsági megoldásai és a rendszer működésének a rendszertervvel történő összehasonlítása alapján történő vizsgálat.

4. A www.webcafeteria.hu rövid áttekintése

Az utóbbi pár évben egyre nagyobb hangsúlyt kapott a cégek munkavállalóinak bérezésében a béren kívüli juttatások (cafeteria) bevezetése, és ezzel együtt egyre nagyobb feladatot jelentett az ezzel kapcsolatok nyilvántartási feladatok elvégzése.

Több vállalkozás készített informatikai rendszert a cafeteria nyilvántartások kezelésére, valamint egyes cafeteria tanácsadók az EXCEL táblákban történő adatnyilvántartást részesítették előnyben, annak a cafeteria rendszerekhez képest számított olcsóságuk miatt.

Több rendszer is, de különösen az EXCEL táblás megoldások sértették az adatvédelmi törvényt, mert az adatok kikerültek a munkáltatók kezeléséből[1].

2008. év elején felmerült az igény egy olyan cafeteria nyilvántartó rendszer elkészítésére, amely amellett, hogy olcsón elérhető, teljesíti a szükséges adatvédelmi és adatbiztonsági szempontokat, és emellett könnyű telepíthetőséget és kezelhetőséget biztosít a felhasználóknak.

5. Jogi háttér

A www.webcafeteria.hu rendszere az alábbi, a vizsgálat időpontjában hatályos jogszabályokon alapul:

1992. év LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

1995. CXVII Szja tv. 69 § 71§

1995. CXVII Szja tv. 1. melléklet

1997. LXXX Tbj 4§

[1] 1992. év LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról

Számvitelről szóló 2000 évi C. tv.

1996. évi LXXXI. tv.

6. Biztonság

a. Regisztráció

A rendszerbe történő regisztráció két lépcsős. A regisztrációt követően a rendszer a megadott email címre egy validálásra szolgáló emailt küld, és az abban található linkre kattintva lesz használható a regisztrált felhasználó. Az email cím beírásakor a rendszer ellenőrzi az email cím szintaktikai helyességét és létezését. Az eljárás az alábbiakat biztosítja:

- Az email cím helyessége
- Az email cím létezése
- Az email címhez a felhasználónak valóban van hozzáférése

b. Bejelentkezés

A bejelentkezéshez SMS azonosítás szükséges, amely első alkalommal úgy történik, hogy a regisztrációkor megadott – és ellenőrzött – email címre egy véletlenszerűen generált betű-szám kombinációból álló kódot küld a rendszer, amelyet az emailben megadott számra, SMS-ben kell elküldeni. Így biztosítható, hogy a felhasználó SMS száma valós legyen, mert azt nem ő maga adja meg, hanem a mobilszolgáltató rendszere.

A kód a megküldése napján érvényes, éjfélig.

Ha a felhasználó mobilszáma már rendelkezésre áll, email küldésére nem kerül sor, hanem a lejárt kód helyett a rendszer SMS-ben küld újat, amely a küldés napján éjfélig érvényes.

A bejelentkezés SMS-ben történő validálása biztosítja, hogy a felhasználónév és jelszó birtokában sem lehet a rendszerben tárolt adatokhoz hozzáférni, ez csak a felhasználónév, a jelszó és a felhasználó mobiltelefonjának egyidejű birtoklása esetén lehetséges.

A rendszer három sikertelen belépési kísérlet esetén a felhasználót három óra időtartamra kizárja, következő bejelentkezés csak a kizárási idő letelte után lehetséges.

A bejelentkezés biztonsága banki szintű.

c. Adatforgalom

Az adatforgalom 1024 bites SSL kommunikációval történik, ami igen erős kódolás, az adatforgalom megfejtéséhez szükséges idő nagyobb, mint az adatok érvényessége, így mire a kommunikációban forgalmazott adatok megfejtése megtörténhet, azok már elavultnak tekinthetők.

A rendszer adatforgalma megfelelően titkosított, **a biztonsága banki szintű**.

d. Adatbiztonság

Az adatbázis biztonságát több intézkedés is szolgálja.

A napi automatikus mentés archiválásra kerül, amelynek őrzése DVD-re írva, hiánytalanul, zárható helyen tárolva történik, így bármikor bármelyik napi mentés tartalma visszakereshető.

Az összes adatokat tartalmazó tábla automatikus változásnaplózással működik. A változás naplózása akkor is megtörténik, ha valaki rendszergazdai jogosultságokkal, az adatbázis közvetlen elérésével módosítja az adatokat. Mivel a változásnapló folyamatos sorszámozású, ennek törlése nem lehetséges nyom nélkül. A változásnapló tárolja a változtatást végrehajtó felhasználó nevét, a változás időpontját, a felhasználó IP címét, az érintett tábla és mező nevét valamint a mező régi és új tartalmát. Több mező egyidejű módosítása esetén a mezők számának megfelelő bejegyzés kerül a változásnaplóba.

Összefoglalásként elmondható, hogy a rendszergazdai jogosultsággal történő módosítás esetén sem kerülhető el a változás naplózása, ami ugyan a módosítás lehetőségét nem zárja ki – a rendszer biztonságos működésének és továbbfejlesztésének érdekében ez nem is javasolt – de bármilyen módosítás esetén megadható a módosítást végző személy, a módosítás időpontja és a módosítás tartalma.

e. Adatvédelem

A www.webcafeteria.hu oldallal kapcsolatos adatkezelést az üzemeltető bejelentette az Adatvédelmi Biztos Hivatalánál. A hivatal által adott nyilvántartási szám:

02713-0001

Az adatvédelmi biztos előzetes állásfoglalása a 9. fejezetben található.

7. A rendszer működése

A rendszer által tárolt és kezet adatok:

- A rendszer használata vagy tesztelése céljából regisztrált cégek adatai
- A rendszer használatára jogosult felhasználók felhasználóneve, jelszava[2], SMS száma és email címe
- A cafeteria rendszerben részt vevő dolgozóknak a munkáltató által kezelt adatai
- számlázáshoz szükséges adatok
- a rendszer működéséhez szükséges adatok (cafeteria partnerek, cafeteria utalványok és ezek kibocsátói, stb.)

A rendszer tesztelése során megállapítottam, hogy a rendszer a specifikációnak megfelelően működik.

Az üzemeltetés során jogszabályváltozások esetén módosítás szükséges, de a legtöbb, jogszabályváltozásból következő módosítás a rendszer paraméterezésével átvezethető, a széleskörű paraméterezhetőségéből következően.

[2] A felhasználók jelszavát a rendszer kódolt állapotban tárolja, annak megismerésére nincs lehetőség

8. Az SSL kódolás

Az **SSL** (Secure Sockets Layer) egy olyan biztonsági protokoll, amelyet Internetes használatra fejlesztettek ki. Amikor megkezdődött az Interneten küldött adatok "lehallgatása", szükségessé vált egy új kódolási eljárás. A banki és kereskedelmi tranzakciók Interneten keresztüli biztonságos lebonyolítása érdekében, ma már nélkülözhetetlen a használata. Működése lényegében arról szól, hogy a küldő fél kódolja a küldendő adatokat, átküldi az Interneten, a fogadó pedig visszafejti. A protokoll egy 40 és egy 128 bites titkosítást is használ. Általában - főleg nemzetközi forgalomban - a 40 bites használata ez elterjedt, holott ez nem nyújt akkora védelmet mint a 128 bites társa, de előnye, hogy gyakorlatilag minden, ma használatos program képes a kezelésére. A 128 bites kulcs olyan ügyfélkörben használatos, ahol mindenki képes vele a dekódolást elvégezni.

Az SSL két részből áll, az egyik a felhasználónál fut a web böngésző részeként (Internet Explorer 3.0 vagy újabb verziók kezelik). A másik pedig a webszerveren, ezek összetettebb funkciókat látnak el. A titkosítási eljárás a nyilvános kulcsú titkosításon alapszik. Létezik egy nyilvános kulcs (a böngészőben), amivel kódolják az adatokat és egy privát kulcs (a szerverben) amivel pedig visszafejtik. A nyilvános kulcsot bárki használhatja, de a dekódolás csak a privát kulccsal lehetséges. Így a küldő (nyilvános kulcs) biztos lehet abban, hogy csak a fogadó képes elolvasni az üzenetet. Visszafelé pedig a nyilvános kulcsot használó biztos lehet abban, hogy a privát kulcs tulajdonosa küldte az adatokat. Az SSL ugyan nem tudja megakadályozni, hogy valaki ellopja menetközben az információt, de az erős kódolás és a kulcsos eljárás révén használhatatlanná teszi a harmadik fél számára.

9. Adatvédelmi biztos állásfoglalása

Ügyszám: 311/K/2008-2.

Ügyintéző: dr. Hegedűs Bulcsú

Tel.: 06-1-47-57-166

Orbán Zoltán

ügyvezető részére

LogiPen Kft.

logipen@invitel.hu

Tisztelt Ügyvezető úr!

Ön beadvánnyal fordult az Adatvédelmi Biztos Irodájához, és munkaügyi adatkezeléssel kapcsolatosan kért állásfoglalást. Beadványa szerint a LogiPen Kft. munkatársai tanácsadás, oktatás és cafeteria utalványoknak a dolgozók részére történő kiosztásával és elszámolásával kapcsolatosan, valamint a Software & Art Kft. munkatársai a webes rendszer fejlesztésével, a rendszert működtető szervez üzemeltetésével, valamint a rendszer használatának oktatásával kapcsolatosan a megrendelő cég dolgozóinak személyes adatait kezelik.

A beadványban ismertetett eljárásban a következő, általános állásfoglalás adható:

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (a továbbiakban: Avtv.) 3. § (1) bekezdése értelmében személyes adat akkor kezelhető, ha ahhoz az érintett személy hozzájárul, vagy ha azt törvény elrendelte.

Az Avtv. 2. § 1. pontja értelmében személyes adat bármely meghatározott (azonosított vagy azonosítható) természetes személlyel (a továbbiakban: érintett) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Az Avtv. 2. § 6. pontja értelmében hozzájárulás az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Az Avtv. 2. § 9. pontja értelmében adatkezelés. az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása.

Az Avtv. 4/A. § értelmében az adatkezelő számára technikai műveletet végző adatfeldolgozó tevékenységéhez az érintett személy hozzájárulása nem szükséges. Az adatfeldolgozó tevékenységét teljes mértékben az adatkezelő határozza meg, önálló döntést a rendelkezésére bocsátott személyes adatokkal kapcsolatosan nem hozhat.

Az Avtv. 2. § 15. pontja értelmében adatfeldolgozás az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Az Avtv. 2. § 19. pontja értelmében harmadik személy olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

A Munka Törvénykönyvéről szóló 1992. évi XXII. törvény - mint szektorális adatvédelmi jogszabály – 3. § (4) bekezdése értelmében a munkavállalóval kapcsolatos személyes adat csak akkor továbbítható harmadik személy számára, ha azt törvény elrendelte, vagy ha ahhoz az érintett munkavállaló hozzájárult.

Az idézett rendelkezések alapján, abban az esetben, ha a munkavállaló személyes adatait a munkáltató harmadik személy számára továbbítja, akkor azt megelőzően az érintett hozzájárulását meg kell kérni. Nem szükséges a hozzájárulás beszerzése akkor, ha az a személy, akinek a munkáltató a személyes adatokat átadja csak technikai műveleteket, vagyis adatfeldolgozást hajt végre.

Az érintett hozzájárulását megadhatja szóban, írásban, vagy hallgatólagosan, ráutaló magatartással. Azt, hogy a hozzájárulás valóban megtörtént utóbb az adatkezelőnek kell bizonyítania.

A beadványában állásfoglalást kért arra vonatkozólag, hogy amennyiben egy munkavállaló az általa használt számítógépen tárolt adatok automatikus biztonsági mentéséhez nem járul hozzá, mit kell tennie az informatikai rendszer szolgáltatójának.

Az ismertetett adatvédelmi rendelkezések értelmében, csak olyan személyes adatok kezelhetők így másolhatók, és tárolhatók, melyek kezeléséhez az érintett munkavállaló hozzájárult.

Beadványában tájékoztatást kért szerzői jogi, illetőleg üzleti adatok felhasználhatóságának kérdésében, tekintettel azonban arra, hogy az Avtv. 1/A. §-a értelmében a törvény hatálya csak természetes személyek adatainak kezelésére terjed ki, a feltett kérdésekben nem áll módomban állásfoglalást adni.

Végezetül, tájékoztatást kért abban a kérdésben, hogy milyen feltételek mellett használható fel az munkaügyi adatbázis marketing célú ajánlatok megtételéhez.

Az Avtv. 5. §-a ismerteti a célhoz kötött adatkezelés elvét. Ennek értelmében személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

Az idézett rendelkezés értelmében, munkaügyi célból létrehozott adatbázis marketing tevékenységre nem használható fel. Az adatkezelés csak akkor tekinthető jogszerűnek, ha a munkavállaló a hozzájárulását adja ahhoz, hogy személyes adatait abból a célból kezelje a munkáltató, vagy harmadik személy, hogy részére reklámokat tartalmazó tájékoztatót küldjenek.

Budapest, 2008. március „ ”

Üdvözlettel:

az adatvédelmi biztos jogkörében eljárva:

Dr. Szabó Máté

az állampolgári jogok országgyűlési biztosa