Deutsches Haus Kft.

Adatvédelmi és Informatikai Biztonsági Szabályzat

Hatályos: 2017. december 1-jétől

DEUTSCHES HAUS
Szolgáltató és
Ingatlanhasznosító Kft.
1062 Budapest, Lendvay u. 22.
Adószám: 11896083-2-42

I. BEVEZETÉS

A Deutsches Haus Kft. (a továbbiakban: Társaság az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Isztv.) foglaltak alapján az alábbi szabályzatot adja ki.

II. ÁLTALÁNOS SZABÁLYOK

1. A szabályzat célja

A szabályzat célja, hogy biztosítsa a Társaság által kezelt adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A szabályzat célja, hogy az informatika alkalmazása során biztosítsa a Társaság tekintetében az alábbiakat:

- az adat-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógép(ek), informatikai eszközök, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- a számítógépes rendszerek zavartalan üzemeltetését,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve azok minimális mértékre csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- adatállományok biztonságos mentését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit.

2. A szabályzat hatálya

2.1 A szabályzat személyi hatálya

E szabályzat személyi hatálya a Társaság ügyvezetőjére terjed ki.

2.2 A szabályzat tárgyi hatálya

E szabályzat tárgyi hatálya kiterjed:

- a Társaság tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre, valamint ezek műszaki dokumentációjára is;
- a rendszer- és felhasználói programokra;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók tárolására, felhasználására;
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

A szabályzat előírásait alkalmazni kell a Társaságnál vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások, illetőleg dokumentumok esetében. A Társaság által nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

III. ÉRTELMEZŐ RENDELKEZÉSEK

1) Adat: a természetes vagy mesterséges objektumok, folyamatok, állapotok jellemzői illetőleg azok részleteinek érzékelhető formában történő megjelenítése. Adat tágabb értelemben jelenthet szöveget, számot, rajzot, térképi részleteket vagy bármely más információt a megjelenési módjára vagy formájára való tekintet nélkül.

2) Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

3) Adatkezelés: az alkalmazott eljárástól függetlenül adatokon végzett bármely művelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, felhasználása, összekapcsolása, szolgáltatása, megjelenítése, stb.

4) Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

5) Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

6) Adatközlő: az a közfeladatot ellátó szerv, amely - ha az adatfelelős nem maga teszi közzé az adatot - az adatfelelős által hozzá eljuttatott adatot honlapon közzéteszi.

7) Adattovábbítás: az adatot meghatározott személy számára történő hozzáférhetővé tétele.

8) Adatvédelem: az adatokhoz való illetéktelen hozzáférés, a meghibásodás, a megsemmisülés, stb. megakadályozása; a személyes adatok esetében kiegészül az adott személy személyes adatai jogellenes gyűjtése, kezelése, tárolása, felhasználása elleni védelemmel.

9) Adattörlés: az adatok felismerhetetlenné tétele olya módon, hogy a helyreállításuk többé nem lehetséges.

10) Információ: jelentéssel bíró adat megjelenési módjára vagy formájára való tekintet nélkül.

11) Kötelezően közzéteendő közérdekű adat: az Isztv 26. § (2)–(3) bekezdésében meghatározott körbe tartozó adat.

12) Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, melynek nyilvánosságra hozatalát vagy hozzáférhetővé tételét törvény közérdekből elrendeli, továbbá közérdekből nyilvános minden, az állami vagyonnal való gazdálkodásra és az azzal való rendelkezésre vonatkozó, közérdekű adatnak nem minősülő adat. Külön törvény az adat megismerhetőségét korlátozhatja

13) Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személye adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

14) Különleges adat: a faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális éltre vonatkozó személyes adat, továbbá az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

15) Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;

16) Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

17) alkalmazói program (alkalmazói szoftver): olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja;

18) felhasználó: az a személy (vagy szervezet), aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához;

19) felhasználói jog: az a jogosultság a hálózaton, amely a felhasználó számára szükséges és elégséges munkájának elvégzéséhez;

20) hálózat: két vagy több számítógép összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé;

21) hardver: az informatikai rendszer eszközeit, fizikai elemeit alkotó része;

22) informatika: a számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működéséhez;

23) informatikai biztonság: olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik, és amelyeket az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni;

24) rendszerprogram (rendszer szoftver): olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk és az alkalmazói programokat működtethessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

25) vírus: önállóan nem működő programrész, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet más, az informatikai rendszerben lévő rendszer- illetve felhasználói programra, sokszorozva önmagát és egy beépített feltételhez kötötten (pl. konkrét időpont) pusztítást indít el.

IV. AZ ADATKEZELÉS, AZ ADATVÉDELEM KÖVETELMÉNY RENDSZERE

4.1. A Társaság szervezeti egysége

A Társaság a feladatai ellátása során kizárólag az adott feladat, a tevékenység megítélése, az adott döntés előkészítése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges – és a személyes adatok körébe tartozó – adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását, irattározását stb. láthatja el.

A Társaság tevékenységének átláthatóbbá tételét szolgáló, illetőleg a jogszabályok által közérdekűnek, közérdekből nyilvános adatnak minősített adatok kezelését, majd ezek közzétételét köteles biztosítani. A közérdekű adatok megismeréséről és közzétételéről külön szabályzat rendelkezik.

Az adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért és szolgáltatásáért.

E szabályzatot a Társaság Szervezeti és Működési Szabályzatával összhangban kell alkalmazni.

4.2. Az adatvédelem tárgya

Az adatvédelem folyamatában a védelem tárgya:

a) a Társaság működése során keletkezett személyes, közérdekű és közérdekből nyilvános adatok teljes köre, keletkezésüktől a megsemmisítésükig,

b) az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, közérdekű, illetőleg közérdekből nyilvános adatokat tartalmaznak. Az adathordozók lehetnek papír alapú iratok, kimutatások, listák, térképek, műszaki dokumentációk, mágneses adathordozók, informatikai rendszerek, hardver, szoftver
c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

4.3. Az adatkezelés alapkövetelményei

A Társaság feladatainak ellátása során biztosítani kell az adatkezelés szabályainak a maradéktalan betartását.

Az adatkezelés során biztosítani kell:

a) az adott egyén szempontjából fontos adatok helyes, pontos kezelését;
b) az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába;

c) a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását;

d) a különböző célú adatok, adatállományok (adatbázisok) folyamatos vezetését, aktualizálást és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára. A személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;

e) a különböző adatok, adatállományok (adatbázisok) valódiságát, pontosságát, részletességét, hitelességét;

f) a különböző adatok, adatállományok (adatbázisok) jellegétől függően azok bizalmas, illetőleg az adott területre vonatkozó jogszabályok szerinti kezelését. A pályázatok, ajánlatok elbírálásáig azok tartalmának zárt – nem nyilvános – kezeléslét;

g) az adatrendszer (akár számítógépes, akár manuális) fizikai biztonságát. Az adatok és az adathordozó eszközök összességében jelentős értéket képviselnek. Megsemmisülésük esetén újra előállításuk többletmunkát és költséget igényel.

4.4 Az adatvédelem eszközei

Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani mindazon igazgatási, iratkezelési, szervezési, személyi, műszaki, technikai, informatikai és egyéb intézkedéseket, melyek elengedhetetlenek az egyes adatok, adatállományok (adatbázisok) zavartalan működéséhez, és védelmet nyújtanak ahhoz, hogy

a) a különböző adatok (adatbázisok) dokumentumok megsérülésére, meghibásodására ne kerüljön sor,

b) az adatkezelés során ismeretek hiánya, hozzá nem értés miatt, emberi mulasztásból károsodásra, adatok, dokumentumok megsemmisülésére ne kerüljön sor.

4.5. Személyi feltételek biztosítása

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Társaság ügyvezetője, mint adatfelelős gondoskodik.
A Társaság ügyvezetője végzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét, és a műszaki ellátást, biztonsági másolatot készít.

4.6. Fizikai, technikai védelem

4.6.1. Tűzvédelem

Az informatikai eszközöket tartalmazó iroda a "D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A tűzvédelemre vonatkozó szabályokat a Tűzvédelmi Szabályzat tartalmazza.

4.6.2. Vagyonvédelem, fizikai biztonság

- az irodahelyiségben elhelyezett számítástechnikai eszközöket csak a kijelölt személyek használhatják;
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős,
- a számítástechnikai eszközöket tartalmazó irodákat minden esetben kulccsal kell zárni.

4.6.3. Adathordozók védelme, tárolása

- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell.

Selejtezendő:

a) a fizikailag sérült, javíthatatlan;
b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott);
c) véglegesen elhasználódott adathordozót.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. Bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

A selejtezést a Selejtezési Szabályzatnak és az Iratkezelési Szabályzatnak megfelelően kell lefolytatni. Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

4.6.4. Adatvédelemi feladatok:

- az adatbevitel hibátlan műszaki állapotú berendezésen történhet;
- csak hibátlan adathordozóra lehet adatállományt rögzíteni;
- adatrögzítő szoftver védelme: a programokat, adatokat ellenőrző funkciókkal, amennyiben szükséges titkosítással kell ellátni.

Az adatállományok file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adattárolókról másolatot kell időnként készíteni.

4.6.5. Vírusvédelem

A számítógépen heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani.

4.6.6. Szoftvervédelem

Az ügyvezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek.

Programhoz való hozzáférés, programvédelem:

a) a kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni;

b) gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek,
c) a feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a programok dokumentációját.

4.6.7. Hardver védelem

- a számítógépeket óvni kell folyadéktól, túlzott páratartalomtól és hőigénybevételtől;
- a számítógép közelében ételt és italt fogyasztani tilos;
- a fali csatlakozók megbontása szigorúan tilos;
- csak földelt aljzatokat lehet használni számítógép üzemeltetéséhez;
- a lengő kábeleket úgy kell elhelyezni, hogy azok balesetet ne okozhassanak, alapelv: sűrűn használt utat szabadon kell hagyni;
- a számítógépek belsejébe nyúlni, és ott bárminemű változtatást okozni tilos, csak az illetékes szakember (informatikus), illetve a szervizek szakemberei nyúlhatnak bele.

4.7. Informatikai védelem

Az irodában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni.

A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépen az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.

A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat.

Védelmi előírások:

- a számítógépe(ke)t csak indítójelszóval lehessen elindítani,
- induláskor minden esetben vírus-ellenőrző programot kell elindítani;
- a feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell;
- a módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni;
- a teljes anyagról heti mentéseket kell készíteni;
- a teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni. Ezeket a törvényekben meghatározott ideig kell megőrizni (pl. adótörvény, társadalombiztosítási törvény, számviteli törvény);
- a felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

V. EGYÉB RENDELKEZÉSEK

A Szabályzatban nem szabályozott kérdésekben az Isztv, az Ibtv., valamint a hatályos jogszabályok rendelkezései az irányadóak.

VI. ZÁRÓ RENDELKEZÉSEK

Jelen Adatvédelmi és Informatikai Biztonsági Szabályzat 2017. december 1. napján lép hatályba.

Budapest, 2017. október 31.

.....

Beck Artúr
ügyvezető

DEUTSCHES HAUS
Szolgáltató és
Ingatlanhasznosító Kft.
1062 Budapest, Lendvay u. 22.
Adószám: 11896083-2-42