TSZI Alapelvek

Jelen TSZI Alapelvek, az átadott dokumentumok útján, vagy egyéb módon, a **Business Case Society Kft**. (a továbbiakban: „**Business Case”**) által megszerzett, az Ügyfél által kezelt, és rendelkezésre bocsátott személyes adatok (együttesen „**Ügyfél Személyes Adat**”) kezelésére vonatkozó, a BUSINESS CASE belső adatkezelési rendszereiben alkalmazott technikai és szervezési intézkedéseket („**TSZIk**”) különösen az alkalmazott elveket, folyamatokat, ellenőrzéseket és eszközöket mutatja be.

1. Jogi Megfelelés

A BUSINESS CASE mindenkor megfelel az adatkezelésre alkalmazandó jogszabályoknak és rendelkezéseknek, különös tekintettel az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló az Európai Parlament és a Tanács (EU) 2016/679 Rendeletének rendelkezéseinek.

2. Adatfeldolgozásra vonatkozó Biztonsági Alapelvek

BUSINESS CASE kiemelt figyelmet fordít az Ügyfél Személyes Adatok védelmének kérdésére. A belső rendszerek, az emberek és a személyes adatok védelme a szervezetet irányító vállalati mechanizmus része. A BUSINESS CASE gondoskodik a megfelelő biztonság megvalósításáról, a hardver- és szoftverkonfigurációk, valamint az üzleti folyamatok és gyakorlatok kialakítása és végrehajtása során. Veszélyforrás, a szervezeten belül vagy azon kívül is kialakulhat, így a BUSINESS CASE biztonsági eljárásaival és gyakorlataival az adatbiztonság számos lehetséges kockázatát mérlegeli, beleértve a technológiai, emberi és természeti tényezőket is. A belső IT biztonsági rendszer kifejlesztésre került. Az IT biztonsági rendszer felügyeleti és ellenőrzési struktúrát biztosít különösen a következők számára: elemzések elvégzése, fizikai biztonság, hozzáféréskezelés, vészhelyzet kezelés, vizsgálatok lefolytatása, információvédelem, oktatás stb.

a) Kompartmentalizáció:

A BUSINESS CASE korlátozza a fizikai és logikai hozzáférést az adatközpontokhoz, így például azon munkavállalókra, akiknek a munkájuk elvégzéséhez elengedhetetlenül szükséges a hozzáférés. A BUSINESS CASE korlátozza az alkalmazásokhoz és az adatbázisokhoz való logikai hozzáférést azon munkavállalókra, akiknek a munkájuk elvégzéséhez elengedhetetlenül szükséges az adatok megismerése.

b) A minimum hozzáférés elve kimondja, hogy egy munkavállaló számára biztosított hozzáférésnek, a munkája elvégzéséhez szükséges minimumra kell korlátozódnia.
c) A feladatok szétválasztásának elve egy olyan alapvető belső kontrol, mely a feladatok összeütközését hivatott elkerülni, olyan módon, hogy egyetlen munkavállalónak sem lehet felhatalmazása vagy hozzáférése ahhoz, hogy a társaság eszközeivel visszaéljen, vagy azok rendszerét megváltoztassa megfelelő következmények nélkül.
d) A Többszintű Védelem arra az eljárásra utal, melynek során a védelem megvalósításához több szintű védelmi rendszert állítanak fel.
e) A beépített adatvédelem azt jelenti, hogy az adatvédelmi elvek már az adatkezelési folyamat megtervezésekor, a Szolgáltatás megkezdésétől kezdve, beépítésre kerülnek a folyamatokba, s azokat a Szolgáltatás teljesítése során mindvégig figyelembe veszik.

3. Fizikai Védelem

3.1. Létesítmény és belépés kontrol

Az Ügyfél Személyes Adat védelmének kulcsfontosságú területe a fizikai védelem. A BUSINESS CASE megfelelő hozzáférés ellenőrző mechanizmusokat alkalmaz a rendszereszközök és az infrastruktúraelemekhez való hozzáférés korlátozásához. Kulcsok, biztonsági zárak, mind példák a BUSINESS CASE által alkalmazott fizikai védelmi rendszerekre.

3.2. Logikai Védelem

A logikai védelmi rendszer elsősorban a következő technikai intézkedésekből áll;

a) Időszakos sebezhetőségi és penetrációvizsgálat.

b) A rendszerek osztályozási struktúráját és a probléma súlyossági szintjét, valamint az operációs rendszer típusát és változatát figyelembe vevő patch-menedzsment elvégzése elvárt időről-időre.
c) Technikai kontrolok a szolgáltatásmegtagadással járó támadások megakadályozására. (elsősorban a hálózati infrastruktúrára és a szerverekre alkalmazandó).
d) Amennyiben az eszköz képes rá, úgy tevékenységnaplórekordok létrehozása és rögzítése (hálózati infrastruktúrára és szerverek), melyek auditálhatóak, s „gyanús tevékenység" figyelő eszközökkel monitorozhatóak.
e) A logikai tűzfalon kívülről, a BUSINESS CASE belső rendszerekhez való távoli hozzáféréshez, különleges biztonsági intézkedések megkövetelése szükséges. Minden ilyen hozzáférés titkosított.
f) Követelmény, hogy az eszközöket ellenőrzési és ellenőrzési célokra használt adatbázisban katalogizálják.
g) Statikus IP-címek használata kötelező (DHCP / DDNS általában nem engedélyezett kivéve néhány jóváhagyott és dokumentált esetet a szerverek, munkaállomások számára). Minden statikus IP-címet egy biztonságos adatbázisban szükséges rögzíteni.
h) A BUSINESS CASE a felhasználók számára elfogadható felhasználási követelményeket tesz elérhetővé, és minden alkalommal figyelmezteti őket az egyes feltételek változására olyan módon, hogy meggyőződhessen arról, hogy a felhasználók elolvasták és megértették az adattárolásra és feldolgozásra vonatkozó követelményeket.
i) Szélesebb körű, független audit eljárás részeként, a biztonsági követelményeknek való megfelelés ellenőrzése követelmény.

3.3. Jelszó és azonosítási elvárások

A BUSINESS CASE belső rendszere megfelelő azonosítást kíván meg belépés előtt. Ez magában foglalja a hálózati eszközöket, szervereket, munkaállomásokat és bizonyos típusú alkalmazásokat is. Egyes rendszerek felhasználói azonosítót és jelszót vagy digitális tanúsítványt, míg mások többfunkciós hitelesítést igényelnek. Többfunkciós hitelesítés szükséges minden olyan rendszerhez, amely elérhető nyilvános hálózat útján vagy bármely hozzáféréssel rendelkező felhasználó számára. Jelszószabályok alkalmazandók. A jelszavaknak meghatározott hosszúságot el kell érniük, s megfelelő betűk, számok és egyéb speciális karakterek kombinációjából kell állniuk. Ezenkívül, a helytelen jelszó szabály értelmében, meghatározott számú próbálkozás után, a hozzáférés megtagadásra kerül. Ahol lehetséges, automatikus eljárások követelik meg a felhasználóktól, hogy megfelelő időközönként megváltoztassák a jelszavaikat, illetve ezen eljárások ellenőrzik a jelszószabályok megtartását.

3.4. Adatbázis biztonság

A BUSINESS CASE kiterjedt és részletes műszaki specifikációkat alkalmaz az adatbázisok biztonsági beállításaihoz. Adatbázisokhoz, mint ahogyan általában a szerverekhez, fizikai és logikai kontrolmechanizmusok kapcsolódnak. Az adatbázisok több szintű hozzáférési rendszert igényelnek, amelyek változhatnak az azokban tárolt adatok érzékenysége alapján. Az adatbázis-adminisztrátoroknak, ahogyan a többi magasabb szintű jogosultsággal rendelkező felhasználónak is, magasabb szintű biztonsági elvárásoknak kell megfelelniük, mint az általános felhasználóknak.

3.5. Munkaállomásokra és a hordozható eszközökre alkalmazandó biztonsági előírások

A BUSINESS CASE munkavállalóinak kötelessége meghatározott előírásokat követni az olyan munkaállomások tekintetében, melyeket Ügyfél Személyes Adat kezelésére használhatnak.
Munkaállomások:

a) Korszerű vírusirtóval kell rendelkezniük. A víruskeresés elvégzése kötelező és automatikusan ütemezett;
b) A bejelentkezéshez jelszó szükséges;
c) A billentyű-, vagy képernyőzárat legfeljebb 30 percre szükséges beállítani (néhány esetben 15 percre);
d) Titkosítási opcióval szükséges állítani minden adatbázist, melyen érzékeny információ tárolható;
e) Ha a hordozható eszköz, támogatja a hardver jelszó beállítását, akkor azt mindig be kell kapcsolni, kivéve, ha az eszközön lévő összes adat titkosítva van;
f) Automatikusan frissen kell tartani, biztonsági javításokkal;
g) Nem tartalmazhat nem jóváhagyott vagy nem megfelelő szoftvereket vagy adatokat;
h) Csak előre jóváhagyott nyílt forráskódú szoftvereket használhatók;

i) Telepíteni és működtetni kell a BUSINESS CASE által jóváhagyott ügyfél tűzfalat;
j) Nem használható internetes peer-to-peer fájlmegosztó alkalmazás;
k) Nem engedélyezhető a hitelesítés nélküli vagy nem jóváhagyott hozzáférés egyetlen formája sem;
l) Belső szoftverelosztó rendszerből szükséges beszerezni a jóváhagyott verzióját a BUSINESS CASE által meghatározott szoftvereknek.

BUSINESS CASE fenntartja a jogot bármely BUSINESS CASE üzleti céljaira használt, vagy arra részben használt személyes tulajdonú eszköz (mint például laptop vagy mobiltelefon) lefoglalására.

3.6. Az üzletmenet folytonossága

Minden, a BUSINESS CASE üzletmenet szempontjából kritikus folyamat tekintetében katasztrófa-helyreállítási terv alkalmazandó. Ezen hivatalos tervek dokumentáltak és legalább évente felülvizsgálandók. Az Ügyfél Személyes Adatot is érintő, technikai támogatás problémajelentő- és megoldó rendszer kiemelt jelentőségű és saját katasztrófa-helyreállítási tervvel rendelkezik.

4. Az adatvédelemre vonatkozó foglalkoztatási gyakorlatok

Az Ügyfél Személyes Adat védelme a fent leírt technikai és egyéb feltételek alkalmazásán és az adatokat kezelő munkavállalók magatartásán múlik. A foglalkoztatási gyakorlatok úgy kerültek kialakításra, hogy biztosítsák, hogy minden munkavállaló és alvállalkozó megfeleljen a szükséges előírásoknak és magatartásuk a jogszabályok által megengedett mértékben ellenőrizhető legyen.

4.1. A Felvételi rendszerre és a jogosultság megvonásra vonatkozó eljárások

A jogszabályok által lehetővé tett keretek között, a munkavégzés előtti szűrés háttérellenőrzéseket, az igényelt képzettség igazolását, a hivatalos fényképes igazolvány és az egyéb alkalmazási kritériumok meglétének ellenőrzését foglalja magában. A jogosultság megvonási eljárás megköveteli a hozzáférés teljes megvonását (24 órát nem meghaladó célzott időn belül). Azon munkavállalók, akiknek a jogosultsága megvonásra kerül, kötelesek visszaszolgáltatni minden BUSINESS CASE tulajdont, különösen ideértve, a munkaállomásokat, laptopokat és bármely egyéb kommunikációs eszközt.

4.2. Betanítás és vállalati kultúra

Az új munkavállalók betanítási folyamatának része az IT eszközök használatára és az érzékeny adatok kezelésére vonatkozó oktatás. Minden felhasználó számára kötelező évente részt venni IT Biztonsági és Anti-korrupciós oktatáson.

4.3. Szabályzatoknak való megfelelés

A BUSINESS CASE munkavállalókra magatartási kódex vonatkozik. A magatartási kódex kötelezi a munkavállalókat a magas etikai normáknak és az adatbiztonsági és titkossági követelményeknek megfelelő üzletmenet folytatására. A BUSINESS CASE ösztönzi a munkavállalókat, a szabályellenes vagy etikátlan magatartások, vagy azok gyanújának jelentésére. A munkavállalók számára kötelező a magatartási kódex elolvasása és az annak való megfelelés elfogadása felvételkor, illetve a kódex változásakor minden alkalommal.

4.4. Bizalmas megbeszélés

Az Ügyfél Személyes Adat védelme érdekében, a munkavállalók bármikor kezdeményezhetnek megbeszélést a menedzsment tagjaival. A BUSINESS CASE megfelelő programok létrehozásával biztosítja ezen szabadság érvényesülését, annak érdekében, hogy a potenciális problémák azonosításra kerülhessenek.

BUSINESS CASE fenntartja a jogot jelen TSZI Alapelvek egyoldalú módosítására, a technikai és szervezési feltételek változásának megfelelően.

Budapest, 2019.08.14

Business Case Society Kft.
képviseletében: Ábrahám Zsolt ügyvezető