3/2025. (III. 24.) számú ügyvezetői utasítás

az adatvédelmi és adatbiztonsági szabályzat kiadásáról

Horváth Csilla, a KKM Magyar Diplomáciai Akadémia Kft. (a továbbiakban: Társaság) ügyvezetőjeként a Társaság mindenkor hatályos Szervezeti és Működési Szabályzata alapján, a munka törvénykönyvéről szóló 2012. évi I. törvény 17. §-ára is tekintettel a következő utasítást adom ki.

1. A Társaság adatvédelmi és adatbiztonsági szabályzatát az 1. számú mellékletben foglaltak szerint határozom meg.

2. A jelen utasítás a kihirdetése napján lép hatályba, és hatálybalépésével egyidejűleg hatályát veszti a 2023. október 1. napjától hatályos adatvédelmi és adatbiztonsági szabályzat.

Budapest, 2025. március 24.

KKM Magyar Diplomáciai Akadémia
Korlátolt Felelősségű Társaság
1107 Budapest, Ceglédi utca 2.
Cégjegyzékszám: 01-09-203215
Adószám: 14163741-2-42
Banksz.: 10300002-13530233-00014905

Horváth Csilla
ügyvezető
KKM Magyar Diplomáciai Akadémia Kft.
Munkáltató

Melléklet:

1. számú melléklet: A Társaság adatvédelmi és adatbiztonsági szabályzata

1. számú melléklet

KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Hatályos: 2025. év március 24. napjától

jóváhagyta:

Horváth Csilla
ügyvezető

KKM Magyar Diplomáciai Akadémia
Korlátolt Felelősségű Társaság
1107 Budapest, Ceglédi utca 2.
Cégjegyzékszám: 01-09-203215
Adószám: 14163241-2-42
Bankszámlaszám: 10300002-13539253-00014905

1. A szabályzat célja, hatálya

1.1. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/A. § (3) bekezdése alapján jelen szabályzat (a továbbiakban: Szabályzat) célja a KKM Magyar Diplomáciai Akadémia Kft. (a továbbiakban: **Társaság**) adatvédelmi és adatkezelési politikájának rögzítése a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETÉBEN (a továbbiakban: GDPR) foglalt elvek figyelembe vételével, amely által a Társaság valamennyi szolgáltatásának igénybevétele során biztosítja az érintettek személyes adataikhoz fűződő jogát azok kezelése, illetve feldolgozása során.

1.2. A Szabályzat tárgyi hatálya kiterjed a Társaság által folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely a Szabályzat értelmező rendelkezéseiben rögzített személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, adatfeldolgozás teljesen vagy részben automatizált eszközzel, illetve manuális módon történik. A Szabályzat személyi hatálya kiterjed a Társaság által foglalkoztatott valamennyi munkavállalóra.

1.3. A Szabályzatot a Társaság a honlapján (www.mdakft.hu) közzéteszi.

1.4. A Társaság a Szabályzat függelékeként közzéteszi az alkalmazott információbiztonsági intézkedéseket, megoldásokat.

2. Értelmező rendelkezések (a GDPR és az Infotv. fogalomrendszerében)

a) **Személyes adat:** azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

b) **Egészségügyi adat:** egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

c) **Bizalmas információ:** olyan adat vagy információ, amely a Társaság számára értékes, és amelyet a Társaságon kívüli személyek általános nem ismernek, ideértve, de nem kizárólagosan, az alábbiakat:
   - kutatás, fejlesztés, architektúra, vázlat, forráskód, objektumkód, szabadalmak, szabadalmi kérelmek, dokumentáció, üzleti titkok, eljárások, találmányok, műszaki adatok, szoftverek, üzleti tervek vagy stratégiák, valamint a Társaságra vagy annak bármelyik munkavállalójára az ügyfél által rábízott információk
   - adatfeldolgozás, forráskódok, számítógépes szoftverek,
   - az üzleti tevékenység során alkalmazott technológiai újítások,

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- minden olyan információ, amelyet az ügyfél harmadik felektől bizalmasan (titoktartási vagy hasonló kötelezettségvállalás hatálya alatt) kapott, valamint az ügyfél és harmadik felek közötti tárgyalások vagy bizalmas szerződések feltételei,
- bármilyen információ, amelyet a Társaság időről időre az ügyfél megbízása során kapott, amelyhez hozzáfér, vagy amelyről más módon tudomást szerzett.

d) **Különleges adat:** a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

e) **Adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

f) **Adatkezelés:** az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

g) **Az érintett hozzájárulása:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

h) **Adatfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

i) **Harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

j) **Adatvédelmi incidens:** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

3. Az adatkezelő adatai

Az adatkezelő megnevezése: KKM Magyar Diplomáciai Akadémia Kft.
Székhelye: 1107 Budapest, Ceglédi utca 2.
Adószáma: 14163241-2-42

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Cégjegyzék száma: 01 09 203215
E- mail címe: info@mdakft.hu
Adatvédelmi tisztviselője: dr. Molnár-Friedrich Szilvia
Adatvédelmi tisztivelő elérhetősége: adatvedelem@mdakft.hu

4. Általános adatkezelési szabályok, alapelvek

4.1. A Társaság tevékenységével összefüggésben megvalósított adatkezelései a feladat- és hatáskörét, működését meghatározó ágazati jogszabályok törvényi felhatalmazásán, valamint az érintettek hozzájárulásán alapulnak. A törvényi felhatalmazás alapján kezelt személyes adatok körét, kezelésének időtartamát az adott ágazati jogszabály (így különösen, de nem kizárólagosan az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, a felnőttképzésről szóló 2013. évi LXXVII. törvény, a munkavédelemről szóló 1993. évi CXIII. törvény, valamint a munkaköri, szakmai, illetve személyi higiénés alkalmassági orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet) határozza meg.
Az érintett önkéntes hozzájárulásán alapuló adatkezelések esetében az érintettek e hozzájárulásukat az adatkezelés bármely szakaszában visszavonhatják. A hozzájárulást az érintett jelen Szabályzat megismerését követően történő kifejezett elfogadásával – az erre vonatkozó jelölőnégyzet kipipálásával – továbbá a weboldal használatával, a weboldalon történt regisztrációval adja meg. A regisztráció során kötelezően megadott adatok kezelése a regisztrációval kezdődik, és – törvény eltérő rendelkezésének hiányában – annak törléséig tart.

4.2. A Társaság magára nézve kötelezőnek ismeri el és alkalmazza a GDPR II. fejezet 5. cikkében foglalt alapelveket, ennek megfelelően tevékenységével összefüggésben az informatikai eszközöket úgy működteti, hogy biztosítja az adatok:

- rendelkezésre állását: az adatnak az arra feljogosítottak számára hozzáférhetőségét,
- bizalmasságát: a jogosulatlan hozzáférés elleni védelmet,
- adattakarékosságát: csak az adatkezelés céljának megvalósításához szükséges adatok kezelését,
- pontosságát: az adatok naprakészségét, a pontatlan személyes adatok törlését,
- integritását: megfelelő technikai intézkedések alkalmazását annak érdekében, hogy az adat jogosulatlan vagy jogellenes kezelés, elvesztés vagy megsemmisítés, károsodás elleni védelme biztosítva legyen.

4.3. A weboldalon tett látogatások során egy vagy több cookie-t – apró információcsomagot – küld a szerver az érintett böngészőjének, mely révén az érintett böngészője egyedileg azonosítható lesz. Ezen cookiek kizárólag a felhasználói élmény javítása, a belépési folyamat automatizálása, valamint a Társaság reklámtevékenysége hatékonyságának mérése érdekében működnek.

5. Szervezeten belüli felelősségek, munkavállalók kötelezettségei, adatbiztonság

5.1. A személyes adatok célhoz kötöttségének elve alapján, az egyes eljárások során kezelt adatokat csak az adott ügy elintézése érdekében szabad felhasználni, más eljárásokkal, illetve adatokkal nem kapcsolhatók össze, kivéve, ha törvény kifejezetten megengedi vagy előírja, illetve az érintett hozzájárult és az adatkezelés feltételei minden egyes személyes adatra vonatkozóan fennállnak.

5.2. Személyes adatokhoz való hozzáférést csak a Társaság feladatkörében érintett munkavállalójának lehet adni, a feladatellátás végrehajtásához szükséges mértékig, azonban az azokat közzétenni, harmadik személy részére hozzáférhetővé tenni tilos, kivéve, ha erre a Társaságot jogszabály kötelezi vagy teszi lehetővé, illetőleg bírósági határozat vagy egyéb hatósági döntés előírása esetén.

5.3. A Társaság az informatikai rendszer üzemeltetése érdekében – jogszabályokban meghatározott keretek között – jogosult adatfeldolgozót igénybe venni a feladatellátása során.

5.3. Az adatminőség biztosítása céljából az adatfelvétel és a további adatkezelés folyamán ügyelni kell a személyes adatok felvételének és kezelésének törvényességére, pontosságára, teljességére és – amennyiben az adatkezelés céljára tekintettel szükséges – időszerűségére, továbbá megfelelő tárolására, illetéktelenek számára hozzáférhetetlenné tételére.

5.4. A célhoz nem kötött, és olyan adatokat, amelyek adatkezelési célja megszűnt vagy módosult, haladéktalanul, illetve az előírt megőrzési határidő leteltével meg kell semmisíteni és az adatkezelést megszüntetni. A személyes adatokat (is) tartalmazó iratanyagok megsemmisítéséről a szükséges biztonsági intézkedések megtartásával kell gondoskodni. Az elektronikus úton rögzített adatokat, ha adatkezelési céljuk megvalósult, további felhasználásuk megakadályozása érdekében felismerhetetlenné, hozzáférhetetlenné kell tenni.

5.5. Az adattörlés maradéktalan megvalósítása érdekében az irattározásra kerülő anyagok selejtezési rendjét a Társaság Iratkezelési Szabályzata határozza meg.

5.6. Személyes adatokat is tartalmazó iratot vagy más adathordozót a Társaság helyiségeiből kivinni – munkaköri feladat ellátásának kivételével – csak indokolt esetben a felettes vezető egyetértésével lehet. A munkavállaló ez esetben is köteles gondoskodni arról, hogy az irat ne vesszen el, ne rongálódjon vagy semmisüljön meg, és tartalma illetéktelen személy tudomására ne jusson.

5.7. Adatvédelmi incidens bekövetkezte esetén az incidens megtörténtét és körülményeit minden munkavállaló köteles haladéktalanul jelenteni a felettes vezetőjének.

5.8. Munkavállalónál tartott, vagy irattárba helyezett iratba az adat megismerésére jogosult személyen kívül más személy csak akkor tekinthet be, ha ezt jogszabály, vagy jogi kötelezettség teljesítése lehetővé teszi. A betekintési jog gyakorlása során úgy kell eljárni, hogy ez által az érintettek személyes adati védelméhez való joga ne sérülhessen. Jelen pont rendelkezéseit a másolat és kivonat készítésére is alkalmazni kell.

5.9. A munkavállaló a nála levő iratokat köteles munkaidőn túl – amennyiben lehetséges, munkaidőben is – elzárt helyen tartani. Munkaidőben személyes adatot tartalmazó iratok csak munkavégzés céljából és a munkavégzéshez szükséges időtartamban lehetnek a

Főv.Törv.szék Cégb.Cg.: 01 09 203215

munkavállalónál.

5.10. A munkavállalók irodai helyiségüket és irat tárolására használt berendezéseket munkaidőben fokozott gondossággal kötelesek ellenőrizni. A munkavállaló köteles a munkaállomását és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végén a számítógépét kikapcsolni vagy alvó állapotba helyezni és, ahol a mágneskártyás fizikai védelem nem megoldott, az irodahelyiségét kulcsra zárni.

6. Az egyes adatkezelésekre vonatkozó különös szabályok

6.1. A munkavállalók személyes adatainak kezelése

6.1.1. A Társaság munkavállalóinak személyes adatait a munkaviszony, munkavégzésre irányuló jogviszony (a továbbiakban együttesen: munkaviszony) létesítésével, teljesítésével és megszüntetésével, valamint a munkaviszonyból származó jogok gyakorlásával és kötelezettségek teljesítésével összefüggésben és az adatvédelem elveinek figyelembevételével kezeli. A munkavállaló személyes adatainak kezelésére más célok tekintetében a GDPR 6. cikkében meghatározott jogalapok szerint kerülhet sor.

6.1.2. A Társaság a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A Társaság ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete – különös tekintettel a személyes adatok különleges kategóriáira – nem ellenőrizhető, kivéve adott esetben a külön jogszabály által szabályozott, erre kijelölt szervek által lefolytatott nemzetbiztonsági ellenőrzés esetét. A Társaság előzetesen tájékoztatja a munkavállalót azokról az eljárásokról, valamint technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

6.1.3. A munkavállaló munkavégzéshez szükséges belépési, betekintési és hozzáférési jogosultságait a munkaköri leírásában foglalt feladatok teljesítéséhez szükséges mértékben kell megállapítani.

6.1.4. A Társaság a munkaviszonyból eredő jogok gyakorlása és kötelezettségek teljesítése érdekében a munkavállalók alábbi személyes adatait kezeli:

a) név,
b) születési név,
c) születési hely, idő,
d) állampolgárság,
e) anyja neve,
f) lakcím,
g) tartózkodási hely,
h) adóazonosító jel,
i) TAJ szám,
j) személyi igazolvány szám,
k) diplomata útlevél adatai,
l) bankszámla neve, száma, számlavezető pénzintézet neve,
m) telefonszám,

Főv.Törv.szék Cégb.Cg.: 01 09 203215

n) e-mail cím,
o) végzettség, szakképzettség megnevezése és okiratszáma,
p) biztosítási jogviszonyt igazoló dokumentumban található személyes adatok,
q) a foglalkozás-egészségüggyel kapcsolatos olyan egészségügyi adatot, amely igazolja, hogy a munkavállaló az adott munkakör betöltésére és ellátására egészségileg alkalmas,
r) nemzetbiztonsági ellenőrzéssel kapcsolatos eredmény.

6.1.5. A Társaság a munkára való alkalmasság vizsgálata keretében a munkavállalók alábbi személyes adatait kezeli:

a) név,
b) születési idő,
c) munkakör,
d) a vizsgálatot végző orvos által írásban rögzített, a foglalkoztatást esetlegesen érintő egyéb megjegyzés,
e) az a tény, hogy a munkavállaló az adott munkakörre alkalmas-e.

6.1.6. Az ügyvezető – figyelemmel a munkavédelemről szóló 1993. évi CXIII. törvény 49. § (1a) bekezdésére – külön utasításban határozza meg azokat a hatásokat, amelyekre figyelemmel a munkaköri alkalmassági vizsgálat kötelező a Társaság egyes munkavállalóira.

6.1.7. A Társaság a munkavállalók számára esetlegesen biztosítható gyermeknevelési támogatás keretében az alábbi személyes adatokat kezeli:

a) munkavállaló neve,
b) születési idő, hely,
c) adóazonosító jel,
d) gyermek neve,
e) gyermek születési ideje,
f) gyermek lakcíme,
g) – tanulói jogviszony esetén – a gyermek oktatási intézményének neve,
h) – tanulói jogviszony esetén – a gyermek oktatási intézményének címe,
i) az a tény, hogy a gyermek a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló törvény alapján fogyatékossági támogatásra nem jogosult, de saját nevelésű igényű tanuló,
j) az a tény, hogy a gyermek fogyatékkal él-e,
k) az a tény, hogy a gyermek köznevelési intézmény tanulója-e,
l) a gyermek születési anyakönyvi kivonatának másolata,
m) örökbefogadás esetén a gyermek örökbefogadását engedélyező döntés, gyám esetén a gyámrendelésről szóló közokirat másolata,
n) 16. életév betöltését követő tanévtől a gyermek tanulói jogviszonyának igazolása érvényes diákigazolvány másolatával, vagy az azt helyettesítő OKTIG rendszerből kiállított QR kódos igazolás,
o) gyermekét egyedül nevelő munkavállaló esetén az emelt összegű családi pótlék folyósításáról szóló határozat másolata,
p) a gyermek fogyatékosságát igazoló szakértői vélemény,
q) sajátos nevelési igényt igazoló szakértői vélemény,
r) amennyiben a munkavállaló a gyermek szülőjének vagy gyámjának a közös háztartásban

Főv.Törv.szék Cégb.Cg.: 01 09 203215

élő házastársa vagy élettársa, a közös háztartásban élő házastársa vagy élettársa lakcímkártyájának másolata.

6.1.8. Amennyiben a 6.1.7. pont l)-r) alpontokban említett dokumentumok egy kérelem benyújtása során már a Társaságnál vannak, azokat a Társaság – a vonatkozó jogszabályok rendelkezéseire figyelemmel – addig kezeli, amíg a munkavállaló kifejezetten nem rendelkezik az adatkezelés megszüntetéséről.

6.1.9. A Társaság a munkavállalók számára esetlegesen biztosítható iskolakezdési támogatás keretében az alábbi személyes adatokat kezeli:

a) munkavállaló neve,
b) születési idő, hely,
c) adóazonosító jel,
d) gyermek neve,
e) gyermek adóazonosító jele,
f) gyermek anyja neve,
g) gyermek születési helye, ideje,
h) gyermek oktatási intézményének neve, címe, évfolyama,
i) 16. életév betöltését követő tanévtől a gyermek tanulói jogviszonyának igazolása érvényes diákigazolvány másolatával, vagy az azt helyettesítő OKTIG rendszerből kiállított QR kódos igazolás.

6.1.10. A Társaság a munkavállalók számára esetlegesen biztosítható szociális célú juttatás keretében a munkavállalók alábbi személyes adatait kezeli:

a) név,
b) munkakör,
c) szervezeti egység,
d) munkaviszony kezdete,
e) igényelt szociális juttatás összege,
f) havi munkabére (bruttó és nettó összegben),
g) a kérelmet alátámasztó indokolás,
h) a kérelmet alátámasztó indokoláshoz kapcsolódó dokumentumok.

6.1.11. A Társaság a munkavállalók számára béren kívüli juttatásokként biztosítható kifizetések tekintetében az alábbi személyes adatokat kezeli:

a) név,
b) adóazonosító jel,
c) az a tény, hogy a munkavállaló részesült-e a személyi jövedelemadóról szóló 1995. évi CXVII. törvény 71. § (1) bekezdés szerinti juttatásban,
d) – amennyiben részesült a c) pont szerinti juttatásban –, a juttatás összege forintban meghatározva.

6.2. Az álláspályázatra jelentkezők személyes adatainak kezelése

6.2.1. A Társaság az álláspályázatra jelentkezők személyes adatait az álláspályázatra történő felhívás és kiválasztási folyamat során kezeli.

Fővtörv.szék Cégb.Cg.: 01 09 203215

6.2.2. Az álláspályázatra történő jelentkezés önéletrajz – esetlegesen motivációs levél – elküldésével kezdődik, vagy munkavállalói ajánlás, illetve munkaerő-kölcsönzés útján. A kiválasztás során személyes vagy telekommunikációs eszköz útján lebonyolított megbeszélésre kerül sor, illetve meghatározott munkakörök esetében az álláspályázónak tesztfeladatot kell megoldania, amely alapján az álláspályázó felkészültsége felmérhető.

6.2.3. A Társaság az álláspályázók alábbi személyes adatait kezeli:

a) név,
b) e-mail cím,
c) telefonszám,
d) szakmai életútra vonatkozó adatok (munkahelyek, munkakörök, készségek kompetenciák),
e) motivációs levél tartalma,
f) a felvétel során esetlegesen keletkező egyéb adatok.

6.2.4. Az álláspályázatra jelentkezők személyes adatai kezelésének jogalapja a GDPR 6. cikk (1) bekezdés b) pontja.

6.2.5. A Társaság az álláspályázatra jelentkezők személyes adatait – a felvett álláspályázó kivételével – a kiválasztási folyamat végéig kezeli.

6.2.6. A Társaság az álláspályázatra jelentkezők számára is hozzáférhetővé teszi a központi honlapján (www.mdakft.hu) az adatkezelési tájékoztatót, így az érintettek a jelentkezést megelőzően megismerkedhetnek annak tartalmával. Amennyiben az álláspályázat munkaerő-toborzó cégen, vagy munkaerő-közvetítőn keresztül érkezik, a Társaság gondoskodik róla, hogy a dokumentumok megküldése előtt az érintett megismerhesse az adatkezelési tájékoztatót.

6.2.7. Amennyiben az álláspályázat belső ajánlás útján érkezik, az ajánlást adó munkavállaló a pályázati anyag elküldését megelőzően tájékoztatja az ajánlott személyt arról, hogy az adatkezelési tájékoztatót a Társaság központi honlapján (www.mdakft.hu) megtalálja. Az ajánlás elküldését követően az ajánlást adó munkavállaló gondoskodik arról, hogy a Társaság eszközeiről pályázati anyag és az arról készült másolatok törlésre kerüljenek.

6.2.8. Az álláspályázat elbírálásában résztvevő személyek gondoskodnak arról, hogy a jelentkezők által benyújtott pályázati anyag és az arról készült másolatok a felvételi eljárás lezárását követően 7 (hét) napon belül törlésére kerüljön. Amennyiben a jelentkező hozzájárulását adta, önéletrajzaik 6 (hat) hónapig újabb állásajánlatok küldése céljából megőrizhetők.

6.2.9. A Társaság álláspályázók személyes adatainak kezelését érintő körülmény, hogy ezen adatok hiányában az álláspályázat érdemben nem bírálható el, ez a kiválasztási folyamat előfeltétele.

6.3. A szerződő felek személyes adatainak kezelése

6.3.1. A Társaság kapcsolattartás és teljesítés céljából kezeli a beszerzési és közbeszerzési

Főv.Törv.szék Cégb.Cg.: 01 09 203215

eljárásokban érintett ajánlattevők, valamint szerződő felek kapcsolattartóinak, képviselőinek adatait.

6.3.2. A Társaság a szerződő felek alábbi személyes adatait kezeli:

a) kapcsolattartó neve,
b) kapcsolattartó e-mail címe,
c) kapcsolattartó telefonszáma,
d) kapcsolattartó telefaxszáma (ha van).

6.3.3. A szerződő felek személyes adatai kezelésének jogalapja a GDPR 6. cikk (1) bekezdés b) pontja.

6.3.4. A Társaság a szerződő felek személyes adatait a szerződéses kapcsolat végéig kezeli, kivéve, ha a szerződéssel összefüggésben bírósági vagy hatósági eljárás van folyamatban. Ebben az esetben az ügy jogerős lezárásáig tart az adatkezelés.

6.4. A társasági számítástechnikai eszközök ellenőrzési rendje

6.4.1. A munkavállalók a Társaság által munkavégzés céljából rendelkezésükre bocsátott számítástechnikai eszközöket (pl.: laptop, mobiltelefon), az internet-hozzáférést és a munkavégzés céljából biztosított e-mail fiókot kizárólag munkavégzésre használhatják.

6.4.2. A Társaság az információ- és hálózatbiztonság megfelelő szintjének fenntartása és a lehetséges adatvédelmi incidensek megelőzése érdekében határvédelmi rendszert tart üzemben, mely tekintetében a kapcsolódó adatkezelésekről a munkavállalókat tájékoztatja. A Társaság felügyeli az általa mobil munkavégzés céljára biztosított, személyes hordozható eszközökön (pl.: mobiltelefon, laptop) használt elektronikus levélcímet (e-mail fiókot), amennyiben a munkavállaló a levelezést az eszközön használja.

6.4.3. A munkáltatói ellenőrzés során az eszközök, illetve az e-mail fiók vizsgálata minden esetben a fokozatosság elvét betartva történik, melynek legfőbb követelménye, hogy az ellenőrzés ne érintse a munkavállaló magánszféráját. Ennek megfelelően a Társaság nem jogosult közvetlenül ellenőrizni, megismerni a munkavállaló meghajtóinak, adathordozóinak, munkahelyi e-mail fiókjának, böngészési előzményeinek (különösen webhelyek, űrlapokra beírt adatok), SMS-fiókjának, híváslistájának, valamint az online kommunikációra használt alkalmazások teljes tartalmát. Az ellenőrzés során a Társaság kizárólag a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnyal összefüggő adatokba tekinthet be, azonban csak olyan mértékig, amely az ellenőrzés céljához feltétlenül szükséges.

6.4.4. A Társaság jogosult annak ellenőrzésére, hogy a számítástechnikai eszközöket a munkavállaló valóban munkavégzésre használja-e. Munkaviszonnyal összefüggő adatnak minősül a korlátozás betartásának ellenőrzéséhez szükséges adat is. Az ellenőrzés során ezen információk olyan mértékben ismerhetők meg, amely alapján eldönthető, hogy azt a munkavállaló valóban munkavégzésre használja-e az eszközöket.

6.4.5. E-mail fiók ellenőrzése során elsősorban a levél tárgya és a feladó e-mail címe alapján vizsgálandó, hogy az adott üzenet munkaviszonnyal összefüggő-e. A munkaviszonnyal

Főv.Törv.szék Cégb.Cg.: 01 09 203215

összefüggő üzenetek akkor ismerhetők meg, ha azt az ellenőrzés célja kifejezetten szükségessé teszi. A magánjellegű e-mailek tartalmát a Társaság – különösen indokolt eset kivételével – nem jogosult megismerni.

6.4.6. A Társaság által a munkavállaló rendelkezésére bocsátott eszközök ellenőrzésére, és ezzel összefüggésben a munkaviszonnyal nem összefüggő adatok megismerése akkor kerülhet sor, ha

a) azon jogsértő tartalomra utaló körülmény jut a Társaság tudomására,
b) azt információbiztonsági incidens vagy adatvédelmi incidens megelőzése vagy kivizsgálása szükségessé teszi,
c) az eszköz használata károsítja vagy kockáztatja az eszköz integritását,
d) alaposan feltehető, hogy a munkavállaló azt nem a munkaviszonnyal összefüggésben használja.

6.4.7. A Társaság által biztosított eszközök meghajtóit és a munkahelyi e-mail fiókokat kizárólag az ügyvezető által kijelölt személy jogosult ellenőrizni. Az ellenőrzés a vonatkozó adatkezelési szabályok megtartásával, megfelelő dokumentáció mellett, a munkavállaló jelenlétében történhet. Az ellenőrzésről, annak okáról, módjáról, feltételeiről és időpontjáról, valamint a munkavállaló adatkezeléssel kapcsolatos jogainak érvényesítési módjáról a munkavállalót előzetesen írásban tájékoztatni kell. Az ellenőrzés céljának ténylegesnek és valósnak, a Társaság tevékenységéhez, a munkavállaló munkaköréhez igazodónak kell lennie. Az ellenőrzésről jegyzőkönyvet kell készíteni. A jegyzőkönyvet a Társaság 3 (három) évig őrzi meg.

6.4.8. Amennyiben a munkavállaló az ellenőrzésen nem tud részt venni, a fenti tájékoztatás mellett lehetőséget kell biztosítani, hogy meghatalmazottja vagy képviselője legyen jelen az ellenőrzésnél. Amennyiben a munkavállaló nem érhető el vagy nem jelenik meg sem személyesen, sem képviselője útján, akkor távollétében, független harmadik személy jelenlétében is lefolytatható az ellenőrzés, csak és kizárólag abban az esetben, ha annak céljai rendkívül nyomósak és azonnali intézkedést igényelnek.

6.4.9. Amennyiben a munkavállaló az ellenőrzésen nem tud részt venni, a fenti tájékoztatás mellett lehetőséget kell biztosítani, hogy meghatalmazottja vagy képviselője legyen jelen az ellenőrzésnél. Amennyiben a munkavállaló nem érhető el vagy nem jelenik meg sem személyesen, sem képviselője útján, akkor távollétében, független harmadik személy jelenlétében is lefolytatható az ellenőrzés, csak és kizárólag abban az esetben, ha annak céljai rendkívül nyomósak és azonnali intézkedést igényelnek.

6.4.10. Figyelemmel arra, hogy a harmadik személytől érkező üzenetek révén magánjellegű adatok az eszközökre kerülhetnek, a munkavállalónak kilépése esetén utolsó munkanapján törölni kell az általa használt számítástechnikai eszközökről és e-mail fiókjából az esetleges magánjellegű adatokat. A műveletek megtörténtét a munkavállaló az ügyvezető által kijelölt személy részére leadott nyilatkozatban rögzíti. Azonnali hatályú felmondás esetén, az adatok törlését a munkavállaló az ügyvezető által kijelölt személy és egy független tanú jelenlétében végzi el, amelyről jegyzőkönyvet kell készíteni, és ezt a Társaság 3 (három) évig őrzi.

6.4.11. Figyelemmel arra, hogy a harmadik féltől érkező üzenetek révén magánjellegű adatok

Főv.Törv.szék Cégb.Cg.: 01 09 203215

érkezhetnek a munkavállalók postafiókjába, a postafiókok forgalma nem irányítható át.

6.5. Bíróság, ügyészség, nyomozó hatóság vagy más hatóság részére történő adattovábbítás

6.5.1. A bíróság, ügyészség, nyomozó hatóság vagy más hatóság által kért adatszolgáltatás tekintetében a Társaság a megkeresésben foglaltaknak megfelelően, az adott ügyben, a vonatkozó jogszabályok előírásai szerint köteles teljesíteni az adatszolgáltatást.

6.5.2. A megkeresésre adott választ a Társaság köteles megfelelően előkészíteni, szükség szerint közreműködőként bevonni a tulajdonosi joggyakorlót.

7. Az érintettek jogainak biztosítása, jogorvoslati lehetőségek

7.1. Az érintettek jogai

Az érintettet az adatkezelés során, összhangban a GDPR 13-22. cikkében foglaltakkal, az abban meghatározottak szerint és rögzített korlátozásokkal, az Infotv. 14. § alapján megilleti:

- az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (előzetes tájékozódáshoz való jog),
- kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (hozzáféréshez való jog),
- kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (helyesbítéshez való jog),
- kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (az adatkezelés korlátozásához való jog),
- kérelmére személyes adatait az adatkezelő törölje (törléshez való jog).

A Társaság a kérelem beérkezésétől indokolatlan késedelem nélkül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről.

7.2. Jogorvoslati lehetőségek

A jogainak megsértése esetén

- a Társaság adatvédelmi tisztviselőjéhez, vagy
- a lakóhelye vagy tartózkodási helye szerint illetékes törvényszékhez fordulhat, továbbá
- adatvédelmi hatósági eljárást kezdeményezhet (Nemzeti Adatvédelmi és Információszabadság Hatóság, 1055 Budapest, Falk Miksa utca 9-11., 1363 Budapest, Pf.: 9., ugyfelszolgalat@naih.hu)

Főv.Törv.szék Cégb.Cg.: 01 09 203215

1. függelék: a Társaságnál alkalmazott információbiztonsági intézkedések, megoldások

Beépített és alapértelmezett adatvédelem

A KKM Magyar Diplomáciai Akadémia Kft. mint adatkezelő (a továbbiakban: Társaság) a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a rendeletekben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

A Társaság megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

Specifikus intézkedések és előírások

Adatbiztonságra törekvő magatartás a Társaság székhelyén és telephelyein:

- Személyes adatokat tartalmazó dokumentumok, iratok nem hagyhatók felügyelet nélkül az asztalon.
- Munkavégzés során (lehetőleg) csak azok az iratok, illetve dokumentumok lehetnek elöl az asztalon, amelyek az adott munka végzéséhez akkor szükségesek.
- Munkavégzés után minden személyes adatot tartalmazó dokumentumot, iratot és elektronikus adathordozót el kell tenni az asztalokról, és zárt, biztonságos helyen kell tárolni.
- A zárható íróasztalokat és szekrényeket is (amennyiben kulcsra zárhatóak) kulcsra zárva kell tartani, és a kulcsokat biztonságos helyen kell őrizni.
- Megbeszélések után a tárgyalóból minden bizalmas tartalmú dokumentumot, különösen a személyes adatokat tartalmazó iratokat, papírokat, jegyzeteket el kell távolítani. (Ide beleértendők a használt flip-chart papírok eltávolítása, táblák letörlése, stb.)
- Személyes adatokat tartalmazó dokumentumok, iratok másolásakor sem eredeti példány, sem másolat nem maradhat a másolóban.
- Személyes adatokat tartalmazó dokumentumok, iratok csak olyan személyeknek adhatók át, akik munkaköri feladatuknál fogva vagy jogszabályi előírásnak megfelelve jogosultak azoknak az információnak a megismerésére vagy használatára, és az átadó személy erről meggyőződött.
- Elektronikus átviteli út (pl. telefon, fax, e-mail) esetén a bizalmas információkat ajánlott, az üzleti titoknak minősített információkat kötelező titkosítva átvinni.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Amennyiben a személyes adatokat tartalmazó dokumentumok, iratok őrzésére, tárolása már nincs szükség, azokat papírdarálóval azonnal, vagy biztonságos gyűjtés, tárolás után kell megsemmisíteni.
- A személyes adatokat tartalmazó kézi feljegyzéseket, munkapéldányokat, másolati példányokat, stb. ugyanolyan biztonsággal kell kezelni, mint az azokat az információkat tartalmazó eredeti, hivatalos iratokat.

Az asztali számítógépek biztonságos használatának feltételei, üres asztal - üres képernyő szabály

- A számítógépekhez, valamint az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen pontban leírtakat;
- a felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges bizalmas információkat tartalmaz;
- az azonosító és a megfelelő erősségű és titokban tartott jelszó használatával a belépő védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszavát szigorúan védeni kell, és a kezdeti jelszót első bejelentkezéskor meg kell változtatni;
- a felhasználó semmilyen infokommunikációs eszközt nem telepíthet a vállalt elektronikus információs rendszerébe, azok elhelyezését, telepítési módját nem változtathatja meg. Semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat;
- az internetről csak vállalati célból lehet fájlokat letölteni! Tilos fájlletöltő szolgáltatások használata. Tilos jogvédett, illetve illegális tartalmak, fájlok letöltése, tárolása!
- a felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényével a rendszergazdát kell megkeresnie;
- a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára, és semmiképpen se legyen látható az épületen kívülről (ha monitor elhelyezéssel nem biztosítható, akkor sötétítő függöny használatával);
- a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha azt őrizetlenül hagyja;
- a zárolás elfelejtésének esetére jelszóvédett, automatikus zárolást kell beállítani, úgy, hogy az maximum 10 perc várakozást követően zárolja a számítógépet;
- a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd leállítani a munkaállomást;
- vendéget irodában felügyelet nélkül hagyni tilos;
- kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

A hordozható számítógépek (laptopok) biztonságos használatának feltételei:

- A hordozható számítógépek biztonságos használatára érvényesek a számítógépek biztonságos használatára, az előző fejezetben előírt szabályok.

- A hordozható számítógépet extrém hőmérséklet, mágneses tér, magas páratartalom vagy erős füstképződés hatásának kitenni TILOS.
- A számítógépeket működő állapotban szállítani nem szabad. (Ez nem vonatkozik az utazás közbeni használatra.)

Adatbiztonsági szabályok:

- Személyes adatok csak titkosítva tárolhatók a hordozható számítógépeken.
- A hordozható számítógépen lokálisan tárolt adatok rendszeres mentéséről a felhasználó maga köteles gondoskodni. A mentéseknek az adathordozón titkosítva kell tárolni, és az adathordozókat biztonságosan kell tárolni.
- A külső munkahelyen történő feladat elvégzése után a hordozható számítógépeken keletkezett vagy tárolt adatokat a megfelelő a hálózati fájlszerverekre kell menteni, és ezt követően a hordozható számítógépről le kell őket törölni.

Jogosulatlanok általi információhoz való hozzáférések megakadályozása:

- Bel- és külföldi kiküldetésre vitt (munkahelyi és otthoni használaton kívül) utazó kollégák notebookjainak vagy asztali számítógépének titkosítását el kell végezni, ennek alkalmazásáért a felhasználó felelős.
- A hordozható számítógépet csak annak a rendszergazda által beállított felhasználója, a saját bejelentkezésével és jelszavával, a munkavégzés céljára használhatja.
- TILOS a hordozható számítógépet más célra használni, illetve másoknak (pl. családtagoknak, barátoknak, ügyfeleknek) használatra átengedni.
- Különösen ott kell a használatot követően a tárolt adatok törlésére odafigyelni, ahol a hordozható számítógépet megosztva használják.
- Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát.
- A hordozható számítógép rövid idejű elhagyásakor is azonnal zárolni kell a számítógépet, ezzel megakadályozva azt, hogy kívülállók betekinthessenek rendszerbe.
- A rendszergazda által installált jelszavas képernyővédő törlése vagy várakozási idejének megváltoztatása TILOS.

Hordozható számítógépek fokozott vírusveszélye kockázatainak csökkentése:

- A rendszergazda által installált központi vírusvédelmi rendszer használata kötelező.
- Az idegen külső adathordozók (pl. optikai adathordozók, külső merevlemezek, flash drive-ok) vírusmentességét felhasználásuk előtt kötelező megvizsgálni.
- A hordozható számítógép külső hálózatra kapcsolódását (pl. szállodákban, vásárokon, beszállítóknál, otthon) követő használata előtt soron kívüli, teljes gépre vonatkozó vírusellenőrzést kötelező végrehajtani.

Intézkedések, ha a hordozható számítógépet már ellopták, vagy elveszítették:

- Az ellopás, elveszítés tényét a lehető leggyorsabban jelenteni kell a rendszergazdának.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Tájékoztatni kell a közvetlen felettes vezetőt arról (előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve), hogy a berendezés tartalmaz-e bárminemű személyes adatot, vagy a Társaság illetve ügyfelei rendszereihez távoli hozzáférési lehetőséget.
- Ha kiküldetés során a számítógépet a szállodai szobából vagy a szálloda ingatlanján álló gépjárműből lopták el, értesíteni kell a szálloda vezetését.
- Rendőrségi jegyzőkönyvet kell felvetetni lopás esetén.
- Hordozható számítógép ellopása esetén, hogyha az személyes adatot is tartalmazott, azt személyes adatvédelmi incidensnek kell minősíteni, és az annak megfelelő eljárást azonnal el kell indítani.

Mobil informatikai adathordozók biztonságos használata:

- Munkavégzés céljaira csak a rendszergazda által kapott, céges adathordozó használható.
- Az adathordozókat azok feldolgozása és tárolása alatt úgy kell kezelni, hogy biztosítva legyenek elvesztés, megsemmisülés, megsérülés és elcserélés, valamint jogosulatlan hozzáférés ellen.
- Gondosan és elzárva kell a használaton kívüli adathordozókat is tárolni.

A Társaság informatikai hálózatának biztonságos használata

- A hálózaton csak a rendszergazda által biztosított és üzemeltetett informatikai eszközök lehetnek.
- Számítógép-hálózati kábel szomszédos helyiségekbe történő áthúzása TILOS!
- A hálózatba a felhasználók csak a saját belépési azonosítójukat használva jelentkeznek be.
- TILOS a saját azonosító és jelszó átadása másnak.
- A rendszergazda által biztosított eszközöket a vállalati hálózatra csatlakoztatás során egy másik, lokális (vezetékes vagy vezeték nélküli) hálózatra kötve megosztani SZIGORÚAN TILOS!
- Az informatikai rendszer használata otthonról csak korlátozottan, felső vezetői engedéllyel, biztonságos VPN csatornán keresztüli bejelentkezéssel engedélyezhető.
- Az informatika rendszerek távoli eléréssel történő használata során a rendszergazda által beállított biztonsági eljárások, eszközök és beállítások (pl. titkosított csatorna, VPN, stb.) használata kötelező.

Bejelentkezési adatok védelme

1. Egy adott jelszót csak egy helyen szabad használni.
2. A jelszót nem szabad képernyőre, más nyilvános helyre, online tárhelyre vagy a fájlszerverre rögzíteni.
3. Amennyiben egy munkavállaló elmegy a Társaságtól, jelszavát meg kell változtatni, email hozzáférését meg kell szüntetni.
4. A jelszó legalább 8 betűs legyen, legyen benne legalább 1 darab szám is, és lehetőleg ne értelmes szó legyen.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

5. Online jelszógenerátort nem szabad használni, mivel ilyen esetekben a jelszó bekerülhet hackelést segítő adatbázisba.
6. Célszerű a jelszavakat 1 évente megváltoztatni.
7. Amennyiben olyan munkavállalónak van szüksége ideiglenes hozzáférésre a jelszóval védett erőforráshoz, aki a jelszó megismerésére nem jogosult, vele ideiglenesen sem szabad a jelszót megosztani, hanem az arra jogosult munkavállaló lépjen be az adott eszközre a jelszó titkosságának megőrzése mellett.
8. Jelszavakat nem szabad lementeni.

Elektronikai eszközök védelme

1. A számítógépeket jelszavas védelemmel kell ellátni.
2. A képernyők automatikusan sötétedjenek el 10 perc inaktivitás után, és a jelszavas védelem automatikusan kapcsoljon be.
3. Amennyiben ez nem megoldható, a számítógép használatának szünetében a képernyőt le kell zárni.
4. Azokon a területeken, ahol a mágneskártyás fizikai védelem nem megoldott, amennyiben egy irodarészben senki sem tartózkodik, az ajtókat zárni kell.
5. Amennyiben lehetséges, a számítógépek merevlemezét titkosítani kell.
6. A számítógépeket folyamatos vírusvédelemmel és tűzfallal kell ellátni.
7. A számítógépek, eszközök értékesítése előtt a merevlemezt, tárolót biztonságosan kell törölni (wipe), ha ez nem megoldható, akkor meg kell semmisíteni, vagy helyreállíthatatlanul meg kell rongálni.

Fájlszerver (NAS) védelme

1. A fájlszerveren található adatokat titkosított partíciókon kell elhelyezni.
2. Minden felhasználó jelszóval kell tudjon csatlakozzon a fájlszerverre.
3. A NAS tárolási helyére csak az arra feljogosított munkavállalók léphetnek be önállóan, más személyek pedig csak kísérettel.
4. A NAS tárolási helyét kulccsal kell zárni.

Belső meghajtók, fájlmegosztó rendszerek használata

- a belső hálózaton mappát kizárólag az ügyvezető engedélyével a rendszergazda törölhet,
- a munkatársak kizárólag a saját feladatuk ellátásához szükséges mappákat használhatják,
- a közös meghajtón magánjellegű információkat, fényképeket SZIGORÚAN TILOS!
- otthoni munkavégzés során különös figyelmet kell fordítani arra, hogy a belső hálózat fájljait senki más ne tekinthesse meg.

Informatikai szakrendszerek védelme

- a Társaság által üzemeltett szakrendszerek kettős autentikációval vannak ellátva a biztonságos belépést garantálva;

Fővárosi Törvényszék Cégbíróság Cg.: 01 09 203215

- Weboldalak SSL tanúsítvánnyal vannak ellátva

A munkahelyi elektronikus levelezés biztonsági előírásai

- A Társaság az elektronikus levelezési szolgáltatást (e-mailt) csak és kizárólag munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. A szolgáltatást magán célra és egyéb, a munkavégzéssel nem összefüggő célokra használni TILOS.
- Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe.
- A felhasználó saját azonosítójának és jelszavának átadása más felhasználók részére TILOS.
- Helyettesítés és távollét esetén a levelezés továbbításának szabálya beállítható, a válaszlevelek küldése esetében az érintett helyettesítő személy rendszerbeli meghatalmazása a helyes, hivatalos eljárás.
- TILOS a munkahelyi e-mail címmel magánjellegű regisztrációt tenni (pl. közösségi oldalak).
- Az ingyenes levelezőrendszerek (pl. freemail.hu) munkahelyi célú használata TILOS.
- Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

Az E-mailek küldésére vonatkozó irányelvek

- A feladó, mint tulajdonos felelős az E-mail tartalmáért.
- TILOS más nevében e-mailt küldeni, kivéve meghatalmazottak (pl. titkárnő) esetében.
- A leveleket mindig célzottan kell kiküldeni, sosem szükségtelenül nagy elosztási kör számára.
- Nagy adatmennyiségeket lehetőleg csak tömörített formátumú csatolmányként szabad küldeni.
- Személyes adatokat tartalmazó dokumentumok e-mail-en keresztül csak titkosított formában küldhetők.
- Zavaró, félreinformáló levelek küldése, jogtalan megrendelések elindítása TILOS és eljárást vonhat maga után.

Az E-mailek fogadására vonatkozó irányelvek

- A címzett felelős az E-mail tovább-feldolgozásáért és továbbításáért.
- Bizalmas információk (pl. különlegesen személyes adatok) továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről.
- Ismeretlen helyről származó e-mail érkezése esetén (pl. a feladó ismeretlen, vagy a feladó e-mail gyanús) megnyitás nélkül értesíteni kell a rendszergazdát.
- Külső vagy belső e-mail címről érkező, félrevezető tartalmú e-mail-ek esetén azonnal értesíteni kell a rendszergazdát.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- A kapott E-mail mellékleteket először számítógépes víruskeresővel kell átvizsgálni, amennyiben azok pl. futtatható programokat tartalmaznak.

Mobiltelefonok, mobileszközök védelme

- Titkosítatlan WIFI-hez csatlakozni nem szabad.
- Az eszközöket PIN kóddal, jelszóval vagy biometrikus azonosítással (arc, ujjlenyomat) kell védeni.
- Amennyiben az eszköz lehetővé teszi, a szenzitív adatokat tartalmazó appokat PIN kóddal, jelszóval vagy biometrikus azonosítással (arc, ujjlenyomat) kell védeni.

Elektronikai eszközökhöz kapcsolódó további előírások

- Amennyiben lehetséges, titkosított adatkapcsolatot és adattárolást kell alkalmazni. Ha ez nem lehetséges, lehetőleg titkosított fájlokat kell küldeni.
- Fejlesztéshez használt környezetekben éles személyi adatokat nem szabad tárolni.

Vírusvédelemhez kapcsolódó szabályok

A központi vírusvédelmi szoftver alkalmazására vonatkozó szabályok

- A rendszergazda által telepített vírusvédelem nélkül sem hálózati, sem önálló munkaállomás, sem hordozható számítógép nem használható.
- A felhasználó nem akadályozhatja a vírusvédelmi program és részeinek folyamatos futását.
- A felhasználónak kötelessége jelenteni a rendszergazdának, ha észleli, hogy a gépén a vírusvédelmi szoftver nem működik folyamatosan.
- A hordozható számítógépek esetében a vírusminta frissítésről való gondoskodás a felhasználó kötelessége.
- A számítógépen idegen adathordozót csak vírusvizsgálat után lehet használatba venni.
- Aki az adatait és adathordozóit rendszeres vírus ellenőrzés vagy vírusvédelmi intézkedés (vírusirtás) alól kivonja, felelősségre vonható, illetve az abból eredő károkért felel.
- Office dokumentumok esetében kerülni kell a makrók és aktív tartalmak megnyitását, külső forrásból érkező dokumentum esetében pedig nem szabad engedélyezni a makrókat.

Teendők vírusfertőzés gyanúja vagy biztos felismerése esetén

Ha a felhasználó gépén vírus jelenlétére utaló működési zavarok jelentkeznek,– ezt a vírusvédelmi program akár jelzi, akár nem –, a következő lépéseket kell tenni:

- Ne használja tovább vírusos vagy vírusgyanús rendszert!
- Ne változtassa meg a rendszer-állapotot!
- Azonnal jelentse az esetet a rendszergazdának!

Fővárosi Törvényszék Cégbíróság: 01 09 203215

A területek fizikai biztonsági követelményei

Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani.
A Szabályzat tárgyi hatálya alá tartozó területeket az alábbi kategóriák egyikébe kell besorolni:
a) belső terület;
b) védett terület;
c) érzékeny terület.

Belső terület

Belső területnek tekintendők a Társaság bejárata utáni közös használatú helyiségei és folyosói és a tárgyalók, oktatótermek. A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az informatikai munkatárs feladata.

Védett terület

Védett terület valamennyi irodahelyiség.

A védett területeket zárva kell tartani. A védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve, ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

Érzékeny terület

- Érzékeny terület a Társaság elektronikus információs rendszereket koncentráltan tartalmazó helyisége.
- Látogatók belépése az érzékeny területre csak hivatalos célból, ellenőrzötten és kísérővel történhet. A látogatóknak a figyelmét fel kell hívni az érvényben lévő biztonsági előírásokra.
- Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni.
- A belépési naplót a titkárságon kell tárolni.
- Az érzékeny területek elérésére a rendszergazda és az ügyvezető jogosultak. Minden más személy részére az ügyvezető csak esetileg engedélyezheti a belépést.

Fizikai belépési engedélyek

- A Társaságnak össze kell állítania azon személyek listáját, akik jogosultak a védett területre önállóan belépni. A listát az ügyvezető hagyja jóvá.
- Az informatikai munkatárs háromhavonta felülvizsgálja a belépésre jogosult személyek listáját és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

Fővárosi Törvényszék Cégbíróság Cégjegyzékszám: 01 09 203215