

KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság

ADATKEZELÉSI ÉS ADATVÉDELMI TÁJÉKOZTATÓ

a KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság felnőttképzési
tevékenységével összefüggő személyes adatkezeléséhez

Hatályos: 2023. október 4. napjától

jóváhagyta:

KKM Magyar Diplomáciai Akadémia
Korlátolt Felelősségű Társaság
1107 Budapest, Ceglédi utca 2.
Cégjegyzékszám: 1-09-203215
Adószám: 1418-0412-42
Banksz.: 10403181-50526554-48491008

Horváth Csilla
ügyvezető

Budapest, 2023. október 4.

ADATKEZELÉSI ÉS ADATVÉDELMI TÁJÉKOZTATÓ

a KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság felnőttképzési tevékenységével összefüggő személyes adatkezeléseihez

BEVEZETÉS

Jelen Adatkezelési és Adatvédelmi Tájékoztató (Tájékoztató) a KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaságnak (a továbbiakban: Adatkezelő/Felnőttképző) a felnőttképzésről szóló 2013. évi LXXVII. törvény (a továbbiakban: Fktv.) és a felnőttképzési törvény végrehajtásáról szóló 11/2020. (II. 7.) kormányrendelet (a továbbiakban: Vhr.), és a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény(a továbbiakban Nftv) szerinti felnőttképzéssel kapcsolatban megvalósított adatkezeléséről és adatvédelméről nyújt tájékoztatást.

Az Adatkezelő a felnőttképző nyilvántartásban B/2021/0001891 nyilvántartási számmal rendelkezik bejelentett, és E/2021/000167 nyilvántartási számmal engedélyhez kötött felnőttképzési tevékenységére vonatkozóan. A Felnőttképző köteles a nyilvántartási számát a képzéssel kapcsolatos dokumentumokon feltüntetni, arról ügyfeleit és a képzésben résztvevő személyeket tájékoztatni. (Fktv.17.§)

I. AZ ADATKEZELŐ MEGNEVEZÉSE

Név: KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság

Rövidített elnevezés: KKM Magyar Diplomáciai Akadémia Kft.

Székhely és levelezési cím: 1016 Budapest, Ceglédi utca 2.

Céggjegyzékszám: 15 09 072172

Adószám: 14163241-2-42

Telefonszám: +36-70-854-52-03

E-mail: info@mdakft.hu; adatvedelem@mdakft.hu

Adatvédelmi tisztviselői feladatokat ellátja: dr. Molnár-Friedrich Szilvia

II. ADATKEZELÉS

Az Adatkezelő az Ön felnőttképzési tevékenységével kapcsolatban az alábbi adatkezelési tevékenységeket végzi.

II.1. A képzés lebonyolításához kapcsolódó adatok

Kezelt adatok köre:

- a) Az Fktv. 21. § (1) a) és b) pontjaiban meghatározott, a képzésben résztvevő személyre vonatkozó és a képzéssel összefüggő adatok:

- természetes személyazonosító adatok (név, születéskori név, anyja neve, születési hely és idő, lakcím/levelezési cím, állampolgárság, TB szám, telefonszám, és – az oktatási azonosító szám kiadásával összefüggésben – oktatási azonosító szám,
- elektronikus levelezési cím,
- legmagasabb iskolai végzettség,
- idegennyelv-ismeret,
- a képzésbe történő belépésével és a képzés elvégzésével, illetve a képzés elvégzése hiányában a képzésből történő kilépésével kapcsolatos adatok,
- a képzés során történő értékelésével és minősítésével kapcsolatos adatok,
- a képzéssel összefüggő fizetési kötelezettségeivel kapcsolatos adatok (képzési díj és annak költségviselője).

b) A Polgári Törvénykönyvről szóló 2013. évi V. törvény rendelkezéseire is figyelemmel a korlátozottan cselekvőképes kiskorú résztvevő képviselőjében eljáró törvényes képviselőjének adatai (név, születési hely és idő, anyja neve, lakcím, útlevél száma, elektronikus levelezési cím, telefonszám, aláírása).

c) Az Fktv. 16. §-ában és a Vhr. 26. §-ában foglalt adatok.

A résztvevők tekintetében az Fktv. 16. § alapján a felnőttképzőnek az alábbi dokumentumokat kell vezetnie, nyilvántartania:

- a képzésben részt vevő személy 21. § (1) bekezdése alapján kezelt személyes adatait, valamint az oktatás, képzés megkezdéséhez és az abban való részvételhez szükséges feltételeket igazoló eredeti dokumentumokat vagy azoknak a Felnőttképző által hitelesített másolatait, továbbá a bemeneti kompetenciamérést és az előzetes tudásmérést igazoló dokumentumokat,
- a felnőttképzési szerződést, a képzési programot, a képzésnek a képzési program szerinti megvalósítását igazoló dokumentumokat,
- a képzés megvalósításához szükséges személyi és tárgyi feltételek biztosítását szolgáló szerződések eredeti példányát,
- az oktatók foglalkoztatásával összefüggő dokumentumokat.

A Vhr. 26. §-a alapján a felnőttképző az egységes dokumentum részeként vezeti a képzésben részt vevő személyek családi és utónevét, a képzés oktatóinak nevét az általuk oktatott tananyag rész megnevezésével és az ezen adatokban bekövetkezett változást a változás időpontjával.

A Vhr. 26.§-a alapján a haladási napló, amely az egységes dokumentum naprakész adatokat tartalmazó, folyamatosan vezetett része tartalmazza

- a) - kontaktórák foglalkozás esetén: a képzés megtartásának időpontját, témájának megjelölését és rövid leírását, oktatójának nevét és aláírását, képzésen belüli órája sorszámának megjelölését, résztvevőinek aláírásával ellátott jelenléti ívet,
- b) - nem kontaktórák képzés esetén: a képzés teljes időtartamát, témájának megjelölését és rövid leírását, résztvevőjének nevét, a képzés befejezésének dátumát.

d) Statisztika esetében anonizált módon a résztvevő által kitöltött elégedettségi kérdőív.

e) A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 80. § (2c) pontja alapján kezeli a képzésben résztvevő egészségügyi alkalmassági vizsgálata elvégzéséhez szükséges személyes adatait.

Adatkezelés célja:

Az adatkezelő az adatokat célhoz kötötten használja.

- A II.1. a) és b) pontjában foglaltak tekintetében az Fktv. 21. § (1) bekezdésének megfelelően a képzés lebonyolítása, az ahhoz kapcsolódó kapcsolattartás, illetve a felnőttképzési szerződés megkötése (Fktv. 13.§ (1), a tanúsítvány kiállítása és eljuttatása (Fktv.13/B.§),
- a II. 1. c) pont szempontjából a vonatkozó szabályozások (jogszabályok /Fktv., Vhr./ és belső szabályzatok) szerint a belső nyilvántartások vezetése,
- a II. 1. d) pont tekintetében pedig az Fktv 21.§ (1) bekezdésben meghatározott adatok statisztikai célokra – különösen a minőségirányításra, tervezésre figyelemmel – történő felhasználása.

Jogalap:

- a) az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (a továbbiakban: GDPR) 6. cikk (1) c) pont: jogszabály (Fktv. 21. §; Fktv. 13/B.§) kötelezi a felnőttképzőt az Ön adatainak a kezelésére. Amennyiben nem adja meg adatait, nem jön létre a felnőttképzési jogviszony. Az adatok kezelése és megőrzése az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.
- b) GDPR 6. cikk (1) f) pont: az adatkezelő és a törvényes képviselő által képviselt korlátozottan cselekvőképes kiskorú jogos érdeke, hogy a polgári jog szabályainak megfelelően a felek között jogviszony érvényesen létrejöhessen.
- c) GDPR 6. cikk (1) c) pont: jogszabály (Fktv. 16. § és a Vhr. 26. §) kötelezi a felnőttképzőt az Ön adatai kezelésére.

Időtartam:

- a) pontban meghatározott személyes adatot az Fktv. 21. § (5) bekezdése értelmében a Felnőttképző a felnőttképzési szerződés megkötésétől számított nyolcadik év utolsó napjáig kezeli. A jogszabályból fakadó kötelezettség miatt ezen adatkezelések tekintetében az adatok törlésére a megőrzési határidő előtt nincs lehetőség.
- b) pontban meghatározott törvényes képviselő adatait a korlátozottan cselekvőképes kiskorú, mint résztvevő adataira előírt 8 évig (nyolcadik év utolsó napjáig) kezeli.
- c) belső nyilvántartások esetében az adatokat annak keletkezésétől számított nyolcadik év utolsó napjáig kezeli az Fktv. 16. §-ában foglaltakra figyelemmel.
- d) statisztika esetében 8 évig (nyolcadik év utolsó napjáig) kezeli, igazodva az egyéb adatok adatkezelési időtartamához. Adatfeldolgozó: -

Adattovábbítás:

1. Az Fktv. 15. § (1) bekezdés értelmében: A felnőttképző

- a) az oktatás, képzés megnevezésére, jellegére, helyére, óraszámára, első képzési napjára és - a zárt rendszerű elektronikus távoktatás keretében megvalósuló képzés kivételével - befejezésének tervezett időpontjára,
- b) a képzésben részt vevő személyek természetes személyazonosító adataira, elektronikus levelezési címére, valamint legmagasabb iskolai végzettségére,
- c) a képzési díjra vonatkozó adatot szolgáltat a felnőttképzési államigazgatási szerv részére a felnőttképzés adatszolgáltatási rendszerében (FAR).

Az adatszolgáltatási kötelezettségnek legkésőbb a képzés megkezdésének időpontját, az adatokban bekövetkezett változás esetén legkésőbb az adatváltozás keletkezését követő harmadik munkanapig, belső képzés esetén annak a negyedévnek az utolsó napjáig kell eleget tenni, amelyikbe a belső képzés befejezésének időpontja esik. A Kormány felnőttképzési államigazgatási szerveként a Pest Megyei Kormányhivatal az ellenőrzéshez szükséges adatokhoz a felnőttképzés adatszolgáltatási rendszerében hozzáfér. A résztvevő félként való részvételével vagy hozzájárulásával megkötött megállapodás ilyen tárgyú rendelkezése esetében a résztvevő tanulmányi előrehaladásról a Felnőttképző a munkáltatót/más személyt vagy szervezetet kérésére, tájékoztatja (GDPR 6. cikk (1) b) pont – szerződés teljesítése érdekében történő adatkezelés).

2. Az Fktv. 21. § (2) bekezdése alapján: Az Fktv. 21. § (1) bekezdés szerinti adatok statisztikai célra felhasználhatók és statisztikai célú felhasználásra személyazonosításra alkalmatlan módon átadhatók, továbbá a Központi Statisztikai Hivatal részére statisztikai célra egyedi azonosításra alkalmas módon térítésmentesen átadhatók és felhasználhatók.

II.2. Az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés

Kezelt adatok köre:

Levelezési cím, állampolgárság, nem magyar állampolgár esetén a tartózkodásának jogcíme, a jogosító okirat, okmány megnevezése, száma, útlevel/szig. szám, társadalombiztosítási azonosító szám, telefonszám.

Adatkezelés célja:

Az egyedi szerződésekre vonatkozó jogok és kötelezettségek gyakorlása, a FAR rendszerbe való feltöltés/bevitel, a személyazonosság és életkor igazolása, a jelentkezők beazonosítása, a képzés sikeres lezárását jelző Tanúsítvány rendelkezésre bocsátása, a képzéssel kapcsolatos változások jelzése a résztvevők felé, a megfelelő kapcsolattartás biztosítása a képzés befejezését követően is.

Jogalap:

GDPR 6. cikk (1) e) pont: a közfeladat ellátáshoz szükséges.

Időtartam:

A felnőttképzés szervezésének és lebonyolításának idején, majd a felnőttképzési jogviszonyból származó igények elévüléséig.

Adatfeldolgozó: -

Adattovábbítás:

A FAR rendszerben meghatározott adatok továbbíthatók a felnőttképzési államigazgatási szerv részére.

II.3. Számla kiállításával és az elmaradt képzési díj és egyéb, a szerződéssel összefüggő fizetési kötelezettség behajtásával kapcsolatos adatkezelés

Kezelt adatok köre:

- a) A résztvevő állandó lakcíme, költségviselő adatai: neve, lakcíme/székhelye.
- b) A résztvevő, költségviselő lakóhelye/tartózkodási helye, értesítési (kézbesítési) címe (ha lakóhelytől vagy tartózkodási helytől eltér), születési helye és ideje, anyja neve, perbeli cselekvőképessége hiányában törvényes képviselőjének a neve és kézbesítési címe.

Adatkezelés célja:

- a) a szerződésben foglalt képzési díj kifizetésének adminisztrációja, számla kibocsátása.
- b) a díj határidőig meg nem fizetett részének behajtása.

Jogalap:

- a) A GDPR 6. cikk (1) c) pont szerinti adatkezelőre vonatkozó jogi kötelezettség: a 2007. évi CXXVII. törvény (Áfatv.) 169. § e) alapján kezeljük a számla kiállításához szükséges adatokat. A számvitelről szóló 2000. évi C. törvény (Számtv.) 169. § (2) bekezdésében előírt megőrzési határidő előtt ezen adatait nem tudjuk törölni (8 év).
- b) GDPR 6. cikk (1) f) pont: a felnőttképző jogos érdeke, hogy a felnőttképzési szerződés alapján őt megillető díjat az érintett nem teljesítése esetén be tudja szedni, a szükséges jogi eljárásokat meg tudja indítani.

Időtartam:

- a) számlakibocsátástól számított 8 év.
- b) A Ptk. 6.22. § értelmében polgári jogi igények érvényesítésére szolgáló 5 év (az elévülés akkor kezdődik, amikor a követelés esedékessé válik, de az elévülési idő nyugvása, megszakadása esetén hosszabb időtartam is lehet).

Adatfeldolgozó: A kiállított számla esetében a NOVITAX rendszer üzemeltetője.

Adattovábbítás:

- a) NAV felé (Áfa tv. 10. melléklet).
- b) megállapodás alapján a felnőttképző képviseletét ellátó ügyvédi iroda, illetve a követelés érvényesítése során eljáró hatóságok felé.

III. AZ ÖNT MEGILLETŐ JOGOSULTSÁGOK (részletes kifejtését a jelen Tájékoztató melléklete tartalmazza)

1. az átlátható tájékoztatáshoz való jog: jelen Tájékoztatóval az adatkezelő információt nyújt az adatkezelés körülményeiről, vagyis többek közt arról, hogy az Ön személyes adatait ki, milyen célból, milyen alapon és meddig kezeli, valamint, hogy Önt az adatkezeléssel összefüggésben milyen jogok illetik meg, és az adatkezelésre vonatkozó kérdéseivel, panaszával kihez fordulhat;
2. a személyes adataihoz való hozzáférés joga: Ön bármikor megkérdezheti az adatkezelőtől, hogy személyes adatainak kezelése folyamatban van-e, az adatkezelésről teljes körű tájékoztatást kérhet, továbbá kérheti, hogy személyes adatairól másolatot kapjon;
3. személyes adatai helyesbítéséhez való jog: Ön kérheti, hogy az adatkezelő az Ön pontatlan személyes adatait javítsa ki, vagy ha hiányosak, azokat egészítse ki;
4. az adatkezelés korlátozásához való jog: Ön (pl. jogi igények előterjesztése, érvényesítése vagy védelme érdekében) kérheti, hogy személyes adatait az adatkezelő csak tárolja, és más módon ne kezelje;
5. a helyesbítésről, törlésről vagy adatkezelés-korlátozásról tájékoztatott címzettek személyére vonatkozó tájékoztatás: kérésére tájékoztatjuk Önt a hivatkozott címzettekről;
6. adathordozhatósághoz való jog: kérheti, hogy az Ön által az adatkezelő rendelkezésére bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja az adatkezelőtől, vagy – ha ez technikailag megvalósítható – az adatkezelő azokat egy másik adatkezelőnek továbbítsa. Ez a jog csak a hozzájárulás vagy szerződés alapján kezelt adatok vonatkozásában illeti meg Önt, feltéve, hogy az adatkezelés automatizált eszközökkel történik;
7. tiltakozáshoz való jog: Ön bármikor tiltakozhat személyes adatainak kezelése ellen, feltéve, hogy az adatkezelés jogalapja jogos érdek vagy az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
9. automatizált döntéshozatal elleni fellépéshez való jog: kérheti, hogy ne terjedjen ki Önre a döntés hatálya. Ha a jelen tájékoztató nem tartalmaz információkat az automatizált döntéshozatalról, akkor az ez elleni fellépéshez való jog értelemszerűen nem releváns.
10. jogorvoslathoz való jog: jogainak megsértése esetén a felnőttképző adatvédelmi tisztviselőjéhez vagy a Nemzeti Adatvédelmi és Információszabadság Hatósághoz vagy bírósághoz fordulhat. A Felnőttképző adatvédelmi tisztviselője: név: dr. Molnár-Friedrich Szilviatelefon_ +36 30 579 7592, mail: SzMolnar-Friedrich@mfa.gov.hu (A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) 1363 Budapest, Pf. 9. Honlap: www.naih.hu. Magyarországon a pert - az érintett választása szerint - az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindíthatja.)

IV. AZ ADATOKAT MEGISMERŐ SZEMÉLYEK KÖRE

Az adatokat Adatkezelő azon munkatársai jogosultak megismerni, akiknek az adat megismerése és kezelése a munkaköri feladataihoz kapcsolódik. Az adatokhoz hozzáférnek továbbá - kizárólag a képzés idejére – a képzés megbízott oktatói, akik ezen adatokat kizárólag a képzés lebonyolítása érdekében használják, valamint a Pest Megyei Kormányhivatal a Felnőttképzési

Adatszolgáltatási Rendszer vezetőjeként és a Központi Statisztikai Hivatal jogszabály alapján. A felnőttképzési tevékenységére vonatkozó tájékoztatóhoz, valamint a képzési programhoz való hozzáférést az ügyfelek, a képzésben részt vevő személyek és a felnőttképzésért felelős miniszter részére biztosítani (Fktv.17.§).

V. ADATBIZTONSÁG

Az Adatkezelő kötelezi magát, hogy gondoskodik az adatok biztonságáról, megteszi továbbá azokat az intézkedéseket, amelyek biztosítják, hogy a felvett, tárolt, illetve kezelt adatok védettek legyenek, illetőleg mindent megtesz annak érdekében, hogy megakadályozza azok megsemmisülését, jogosulatlan felhasználását és jogosulatlan megváltoztatását.

Kötelezi magát arra is, hogy minden olyan harmadik felet, akiknek az adatokat esetlegesen továbbítja vagy átadja, ugyancsak felhívja ez irányú kötelezettségeinek teljesítésére.

Az adatkezelések során nem történik személyes adatai alapján automatizált döntéshozatal, profilalkotás.

Az Adatkezelő megtesz minden olyan biztonsági, technikai és szervezési intézkedést, amely az adatok biztonságát garantálja.

V.1. Szervezési intézkedések

Az Adatkezelő az informatikai rendszereihez a hozzáférést személyhez köthető jogosultsággal teszi lehetővé. A hozzáférések kiosztásánál érvényesül a „szükséges és elégséges jogok elve”, azaz az Adatkezelő informatikai rendszereit és szolgáltatásait minden felhasználó csak a feladatának ellátásához szükséges mértékben, az ennek megfelelő jogosultságokkal és a szükséges időtartamig használhatja. Az informatikai rendszerekhez és szolgáltatásokhoz hozzáférési jogot csak az a személy kaphat, aki biztonsági vagy egyéb (pl. összeférhetetlenségi) okokból nem esik korlátozás alá, valamint rendelkezik az annak biztonságos használatához szükséges szakmai, üzleti és információbiztonsági ismeretekkel.

V.2. Technikai intézkedések

Az Adatkezelő többszintű, tűzfalas védelemmel védi a belső hálózatát. Az alkalmazott nyilvános hálózatok belépési pontjain mindenhol minden esetben hardveres tűzfal (határvédelmi eszköz) helyezkedik el. Az adatokat az Adatkezelő redundánsan – azaz több helyen – tárolja, hogy védje azokat az informatikai eszköz meghibásodásából fakadó megsemmisüléstől, elvesztéstől, sérüléstől, a jogellenes megsemmisítéstől. Többszintű, aktív, komplex kártékony kódok elleni védelemmel (pl. vírusvédelem) védjük a belső hálózatainkat a külső támadásoktól. Az Adatkezelő által működtetett informatikai rendszerekhez, adatbázisokhoz az elengedhetetlen külső elérést az Adatkezelő titkosított adatkapcsolaton keresztül valósítja meg (VPN) és az Adatkezelő weboldalai SSL tanúsítvánnyal vannak ellátva. Mindent megteszünk azért, hogy informatikai eszközeink, szoftvereink folyamatosan megfeleljenek a piaci működésben általánosan elfogadott technológiai megoldásoknak és naprakészek legyenek. A fejlesztéseink során olyan rendszereket alakítunk ki, amelyekben a naplózás révén kontrollálhatók és nyomon követhetők a végzett műveletek, észlelhetők a bekövetkezett incidensek, például a jogosulatlan hozzáférés. Az Adatkezelő szervere a tárhelyszolgáltató elkülönített dedikált szerverén, védetten és zártan található.

VI. EGYÉB RENDELKEZÉSEK

VI.1. A felnőttképzési államigazgatási szerv az adatokról és a felnőttképző által kiállított tanúsítványról – a Fktv. 20. § (1) bekezdése szerinti ellenőrzés és a pályakövetési rendszer működtetése céljából – elektronikus nyilvántartást vezet, és a nyilvántartás adatait azok keletkezésétől számított ötvenedik év utolsó napjáig kezeli. A felnőttképzési államigazgatási szerv a tanúsítványokat tartalmazó központi nyilvántartás adatait azok keletkezésétől számított ötvenedik év utolsó napjáig kezeli, azt követően pedig azokat átadja az illetékes levéltárnak, és az átadott adatokat törli.

VI.2. A felnőttképzés lebonyolításával kapcsolatban kezelt személyes adatokhoz kizárólag az Adatkezelő férhet hozzá. Amennyiben bíróság vagy más hatóság előtt eljárás indult, amelynek keretében szükségessé válik a személyes adatok továbbítása a bíróság vagy a hatóság felé, úgy abban az esetben a bíróság vagy a hatóság is hozzáférhet a személyes adatokhoz.

VI.3. Minden olyan esetben, ha a szolgáltatott adatokat Adatkezelő az eredeti adatfelvétel céljától eltérő célra kívánja felhasználni, erről Önt tájékoztatja, és ehhez előzetes, kifejezett hozzájárulását megszerzi, illetőleg lehetőséget biztosít számára, hogy a felhasználást megtiltsa.

VI.4. Az Adatkezelő fenntartja magának a jogot, hogy a jelen Tájékoztatót bármikor, egyoldalúan megváltoztassa. Amennyiben a Tájékoztató módosulna, akkor erről az Adatkezelő értesíti az érintetteket.

VI.5. A Tájékoztató elektronikus formában az Adatkezelő honlapján (www.mdakft.hu), illetve papír alapon a székhelyén érhető el.

Az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek részletes ismertetése

Az adatkezeléssel érintett (a továbbiakban érintett) adatkezeléssel összefüggő jogainak és jogorvoslati lehetőségeinek ismerete azért fontos, mert az adatkezelő személyes adatokat kezel. Személyes adatnak minősül minden olyan információ, ami alapján az érintett azonosítható. Így személyes adat nem csak az érintett neve, azonosító jele, hanem akár a fizikai, mentális stb. azonosságára jellemző ismeret is.

Az érintett az adatkezeléssel összefüggő jogai gyakorlása érdekében az adatkezelőhöz fordulhat, aki indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Az alábbiakban az érintettet illető egyes jogok kifejtése olvasható.

1. Átlátható tájékoztatáshoz való jog (GDPR 12-14. cikk)

Az adatkezelő jelen dokumentummal tesz eleget az adatkezelőre, az adatvédelmi tisztviselőre, az adatkezelés céljára és jogalapjára, időtartamára, az érintetti jogokra, és a jogorvoslatra, továbbá ha az adatok nem az érintettől származnak, akkor az adatok forrására vonatkozó tájékoztatási kötelezettségének. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy igazolja a személyazonosságát.

2. Az érintett hozzáférési joga (GDPR 15. cikk)

Az érintett kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, beleértve az adatkezelés tárgyát képező személyes adatok másolatát. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

- a) az adatkezelés céljai;
- b) az érintett személyes adatok kategóriái;
- c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
- d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;
- f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
- g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

3. A helyesbítéshez való jog (GDPR 16. cikk)

Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

4. A törléshez való jog: „ az elfeledtetéshez való jog” (GDPR 17. cikk)

A személyes adatot törölni kell, ha

- 1. az adatkezelés célja megszűnt;
- 2. az érintett visszavonta a hozzájárulását és az adatkezelésnek nincs más jogalapja;
- 3. az adatkezelés jogos érdeken alapul vagy közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az érintett tiltakozik az adatkezelés ellen;
- 4. az adatkezelés jogellenes;
- 5. a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- 6. az adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában került sor.

5. Az adatkezelés korlátozásához való jog (GDPR 18. cikk)

Az adatkezelő az érintett kérésére korlátozza az adatkezelést, ha

1. az érintett vitatja a személyes adatok pontosságát;
 2. az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését;
 3. adatkezelőnek már nincs szüksége a személyes adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
 4. az adatkezelés jogos érdeken alapul vagy közérdekű/az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az érintett tiltakozik az adatkezelés ellen.
6. A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség (GDPR 19. cikk)

Az adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, törlésről vagy adatkezeléskorlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet, kérésére, az adatkezelő tájékoztatja e címzettekről.

7. Adathordozhatósághoz való jog (GDPR 20. cikk)

Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon működik. Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. E jog gyakorlása nem sértheti az elfeledtetéshez való jogot.

8. A tiltakozáshoz való jog (GDPR 21. cikk)

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak jogos érdeken alapuló kezelése ellen, vagy ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, ideértve az említett jogalapokon alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

9. Automatizált döntéshozatal esetén az érintettet megillető jog (GDPR 22. cikk)

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Ez a rendelkezés nem alkalmazandó a következő esetekben:

- a) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;

b) meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy

c) az érintett kifejezett hozzájárulásán alapul.

Az adatkezelő köteles biztosítani az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

10. Jogorvoslat igénybevétele: vagylagosan rendelkezésre álló lehetőségek

10.1. Adatvédelmi tisztviselő (GDPR 38-39. cikk)

Az érintettek a személyes adataik kezeléséhez és a GDPR szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak (GDPR 38. cikk (4) bek.). Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával. (GDPR 12. cikk (4) bek.)

10.2. Nemzeti Adatvédelmi és Információszabadság Hatóságnál kezdeményezhető eljárások (GDPR 57- 58. cikk, 77. cikk, Infotv.7 51/A. (1) bekezdés, 52-54.§, 55.§ (1)-(2), 56-58. §, 60-61. §)

A Nemzeti Adatvédelmi és Információszabadság Hatóságnál (a továbbiakban Hatóság) bejelentéssel bárki (tehát nem csak az érintett) vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll. Fontos, hogy a bejelentés ne legyen névtelen, különben a Hatóság érdemi vizsgálat nélkül elutasíthatja a bejelentést. A további elutasítási indokokat az Infotv. 53. §-a tartalmazza.

A Hatóság vizsgálata ingyenes, a vizsgálat költségeit a Hatóság előlegezi és viseli. Az eljárás lefolytatására vonatkozó részletes szabályokat az Infotv. 54.§, 55. § (1)-(2) bekezdése, 56-58. §-ai tartalmazzák.

A személyes adatok védelméhez való jog érvényesülése érdekében a Hatóság az érintett erre irányuló kérelmére adatvédelmi hatósági eljárást indít az Infotv. 60-61. §-a alapján.

10.3. Bírósági jogérvényesítés (GDPR 79. cikk, Infotv. 23. §,)

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat, mivel minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak a GDPR-nak nem megfelelő kezelése következtében megsértették a GDPR-ban rögzített jogait (lásd.fent).

A pert az adatkezelővel vagy az adatfeldolgozóval szemben, az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

Magyarországon a pert - az érintett választása szerint - az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindíthatja.

Az érintett a perben kártérítést/sérelemdíjat követelhet az adatkezelőtől: - ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak kárt okoz, köteles azt megtéríteni; - ha az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével megsérti az érintett személyiségi jogát (pl. személyes adat illetéktelen személlyel való közlése vagy nyilvánosságra hozatala), az érintett sérelemdíjat követelhet az adatkezelőtől.

KKM Hungarian Academy of Diplomacy Limited Liability Company

**DATA MANAGEMENT AND PRIVACY POLICY OF KKM HUNGARY
ACADEMY OF DIPLOMACY KFT ADULT EDUCATION
PROCESSING OF PERSONAL DATA RELATING TO ITS ACTIVITIES**

Effective: from 4 October 2023

**approved by Csilla Horváth,
Managing Director**

Budapest, 2023.10.04

DATA MANAGEMENT AND PRIVACY NOTICE

for the personal data processing of KKM Hungarian Academy of Diplomacy Limited Liability Company in connection with its adult education activities

INTRODUCTION

This Data Management and Data Protection Informative (Informative) is issued by KKM Hungarian Academy of Diplomacy Limited Liability Company (hereinafter referred to as the "Data Controller/Adult Educator") in accordance with Act LXXVII of 2013 on Adult Education (hereinafter referred to as the "Act on Adult Education") and the Government Decree No. 11/2020 (II. 7.) on the implementation of the Adult Education Act (hereinafter referred to as the "Vhr."), and the Act CCIV of 2011 on National Higher Education (hereinafter referred to as the "Nftv") and informs on the data management and data protection in connection with adult education.

The Data Controller has the registration number B/2021/0001891 in the Adult Education Register for its adult education activities that have been registered and the registration number E/2021/000167 for its adult education activities that are subject to authorisation. The Adult Education Provider is obliged to indicate its registration number on the documents related to the training and to inform its clients and the persons participating in the training about it.

I. NAME OF THE DATA CONTROLLER

Name: the Hungarian Academy of Diplomacy Limited Liability Company

Abbreviated name: KKM Hungarian Academy of Diplomacy Kft.

Registered office and postal address: 1016 Budapest, Ceglédi utca 2.

Company registration number: 15 09 072172

Tax number: 14163241-2-42

Phone number: +36-70-854-52-03

E-mail: info@mdakft.hu; adatvedelem@mdakft.hu

Data Protection Officer undertaking Duties: dr. Szilvia Molnár-Friedrich

II. DATA PROCESSING

The Data Controller carries out the following processing activities in relation to your adult learning activities.

II.1. Data relating to the delivery of the training

Scope of data processed:

- a) Data on the person participating in the training and data related to the training, as defined in Section 21 § (1) a) and b) of the Fktv Act:

- natural person identification data (name, name at birth, mother's name, place and date of birth, address/passport address, nationality, social security number, telephone number, and, in the context of the issue of an education identification number, an education identification number,
 - e-mail address,
 - highest level of education,
 - foreign language skills,
 - data relating to entry into and completion of the training or, if the training is not completed, exit from the training,
 - data relating to the assessment and qualification of the training,
 - details of training-related payment obligations (training fee and the party responsible for paying it).
- b) Subject to the provisions of Act V of 2013 on the Civil Code, the details of the legal representative of the minor participant with limited capacity (name, date and place of birth, mother's name, address, passport number, e-mail address, telephone number, signature).
- c) The data contained in § 16 of the Fktv. and § 26 of the Vhr.

With regard to the participants, the adult education provider must keep and record the following documents pursuant to Section 16 of the Adult Education Act:

- the personal data of the person participating in the training processed pursuant to § (1) of Article 21, as well as the original documents or copies thereof certified by the Adult Education Provider certifying the conditions for commencing and participating in education and training, and documents certifying the entrance competency assessment and the preliminary knowledge assessment,
- the adult learning contract, the training programme, the documents proving the delivery of the training according to the training programme,
- the original copy of the contracts providing the necessary staff and equipment for the training,
- documents relating to the employment of trainers.

Pursuant to § of Article 26 of the Vhr., the adult education provider shall keep as part of the single document the surname and first name of the persons participating in the training, the name of the trainers of the training with the name of the part of the curriculum they teach and the date of the change in this data.

Pursuant to § 26 of the Vhr., the progress logbook, which is the continuously kept part of the single document containing up-to-date data, contains

- a) - in the case of contact hours: the date of the training, a brief description of the subject, the name and signature of the instructor, the number of hours of the training, a signed attendance sheet of the participants,
 - b) - in the case of non-contact training: the total duration of the training, an indication and brief description of the subject, the name of the participant, the date of completion of the training.
- d) In the case of statistics, anonymised satisfaction questionnaire completed by the participant.

e) Pursuant to Section 80 (2c) of Act CCIV of 2011 on National Higher Education, it processes the personal data of the trainee necessary for the performance of the medical fitness examination.

Purpose of processing:

The data controller uses the data for a specific purpose.

- With regard to II.1. a) and b), in accordance with Fktv. 21 § (1) of the Adult Education Act, the provision of training, the related contact and the conclusion of the adult education contract (Fktv. 13 § (1), the issue and delivery of the certificate (Fktv. 13/B. §),
- for the purposes of point II.1. c), keeping internal records in accordance with the relevant regulations (legislation / Fktv., Vhr./ and internal regulations),
- with regard to point II. 1. d), the use of the data specified in 21. § (1) of the Fktv for statistical purposes, in particular with regard to quality management and planning.

Legal basis:

- a) Article 6 (1) c) of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: GDPR): the adult education provider is obliged by law (Fktv. § 21; Fktv. § 13/B. §) to process your data. If you do not provide your data, the adult education legal relationship will not be created. The processing and retention of the data is necessary to fulfil the legal obligation on the Data Controller.
- b) Article 6(1)(f) GDPR: the legitimate interest of the data controller and the minor of limited capacity represented by the legal representative to establish a valid legal relationship between the parties in accordance with the rules of civil law.
- c) GDPR Article 6 (1) (c): the adult education provider is obliged by law (Fktv. § 16 and Vhr. § 26) to process your data.

Duration:

- a) The personal data specified in point (a) shall be processed by the Adult Education Provider until the last day of the eighth year following the conclusion of the adult education contract, pursuant to § (5) of Article 21 of Fktv. Due to the statutory obligation, it is not possible to delete the data before the retention period for these data processing operations.
- b) will keep the data of the legal representative as defined in point (a) for the 8 years (until the last day of the eighth year) required for the data of the minor with limited capacity as a participant.
- c) in the case of internal records, it shall manage the data until the last day of the eighth year following their creation, subject to the provisions of Section 16 of the Act on the Protection of Personal Data.
- d) for statistics, for 8 years (until the last day of the eighth year), in line with the processing period for other data. Data processor.

Data transmission:

1. Pursuant to Section 15 § (1) of the Fktv: The adult education provider

- a) the name, nature, place, number of hours, first day of training and, except in the case of closed e-learning, the planned date of completion of the training,
- b) the trainees' natural identity data, e-mail address and highest educational level,
- c) provide data on the training fee to the adult education public administration in the Adult Education Data Reporting System (FAR).

The obligation to provide the information must be fulfilled no later than the date on which the training starts, or, in the case of a change in the data, no later than the third working day following the date on which the data change occurs, or, in the case of internal training, by the last day of the quarter in which the internal training is completed. The Pest County Government Office, as the adult education state administration body of the Government, has access to the data required for the audit in the adult education data system. In the case of such a provision of an agreement concluded with the participation or consent of the participant, the Adult Education Provider will inform the employer/other person or organisation of the participant's learning progress upon request (Article 6 (1) (b) GDPR - processing for the performance of a contract).

2. Pursuant to § (2) of Article 21 § (1) of the Fktv.: data pursuant to § (1) of Article 21 of the Fktv. may be used for statistical purposes and may be transmitted in a manner that is not suitable for identification for statistical purposes, and may be transmitted to and used by the Central Statistical Office free of charge in a manner that is suitable for individual identification for statistical purposes.

II.2. Processing necessary for the performance of a task carried out in the exercise of official authority vested in the data controller

Scope of data processed:

Address, nationality, in case of non-Hungarian citizenship, title of residence, name and number of the legal document, passport/ID number, social security number, telephone number.

Purpose of processing:

Exercising rights and obligations regarding individual contracts, uploading/entering data into the FAR system, verifying identity and age, identifying candidates, providing a Certificate of Successful Completion of Training, notifying changes to the training to participants, ensuring appropriate contact after the training has been completed.

Legal basis:

Article 6(1) e) GDPR: necessary for the performance of a public task.

Duration:

During the organisation and delivery of adult education and training, and until the claims arising from the adult education and training relationship expire.

Data processor: -

Data transmission:

The data defined in the FAR system may be transmitted to the adult education public administration.

II.3. Processing of data relating to the issuing of invoices and the recovery of unpaid training fees and other contractual payments

Scope of data processed:

- a) Permanent address of the participant, details of the person responsible for the costs: name, address/place of residence.
- b) Place of residence/residence, notification (delivery) address (if different from the place of residence or domicile), date and place of birth, name of the mother, name and service address of the legal representative in the absence of legal capacity of the participant or legal representative.

Purpose of processing:

- a) administering the payment of the training fee, issuing invoices.
- b) exaction of the unpaid part of the fee.

Legal basis:

- a) Legal obligation of the data controller under Article 6 (1) c) GDPR: we process the data necessary for issuing the invoice pursuant to 169 § e) of Act CXXVII of 2007 (Áfatv.). We cannot delete these data before the retention period provided for in 169 § (2) of Act C of 2000 on Accounting (Számtev.) (8 years).
- b) Article 6 (1) f) GDPR: it is in the legitimate interest of the adult education provider to be able to collect the fee due to it under the adult education contract in the event of non-compliance by the data subject, and to initiate the necessary legal proceedings.

Duration:

- a) 8 years from the date of issue.
- b) According to the 6.22 § of the Civil Code, the limitation period for the enforcement of civil claims is 5 years (the limitation period begins when the claim becomes due, but may be longer in the event of the statute of limitations being suspended or interrupted).

Data Processor: in the case of an issued invoice, the operator of the NOVITAX system.

Data transmission:

- a) to NAV (Annex 10 of the Áfatv.).
- b) by agreement with the law firm representing the adult education provider or the authorities responsible for enforcing the claim.

III. THE RIGHTS APPLICABLE TO YOU (explained in detail in the Annex to this Prospectus)

1. the right to transparent information: with this Notice, the data controller provides information about the circumstances of the processing, including who processes your personal

data, for what purposes, on what basis and for how long, as well as your rights in relation to the processing and to whom you can address any questions or complaints about the processing;

2. your right of access to your personal data: you may at any time ask the data controller whether your personal data are being processed, request full information about the processing and obtain a copy of your personal data;

3. the right to rectification of your personal data: you can ask the data controller to correct inaccurate personal data or, if incomplete, to complete it;

4. the right to restriction of processing: you may request that the data controller only stores your personal data (e.g. to establish, exercise or defend legal claims) and does not process them otherwise;

5. information on the identity of the recipients informed of the rectification, erasure or restriction of processing: we will inform you of the recipients concerned at your request;

6. the right to data portability: you may request that the personal data you have provided to the data controller be received by the data controller in a structured, commonly used, machine-readable format or, if technically feasible, transferred by the data controller to another data controller. You have this right only in relation to data processed on the basis of consent or contract, provided that the processing is carried out by automated means;

7. right to object: you may object to the processing of your personal data at any time, provided that the legal basis for the processing is a legitimate interest or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

9. the right to object to automated decision-making: you can ask not to be covered by the decision. If this notice does not contain information on automated decision-making, the right to object is, by definition, not relevant.

10. the right to redress: in the event of a breach of your rights, you can appeal to the Data Protection Officer of the adult education centre or the National Authority for Data Protection and Freedom of Information or to a court. The Data Protection Officer of the Adult Education Centre name: Dr. Molnár-Friedrich Szilvia telephone number: +36 30 579 7592, mail: SzMolnar-Friedrich@mfa.gov.hu (The National Authority for Data Protection and Freedom of Information (NAIH) 1363 Budapest, Pf. 9. In Hungary, the lawsuit may also be brought, at the choice of the data subject, before the courts of the place of residence or domicile of the data subject.)

IV. THE PERSONS WHO HAVE ACCESS TO THE DATA

The data may be accessed by those employees and contractual partners of the Data Controller whose access to and processing of the data necessary for the performance of their duties is related to their job duties and the performance of data communication and data recording tasks in accordance with the legal requirements. The data may also be accessed, for the duration of the training only, by the instructors of the training, who use the data solely for the purposes of the training, by the Pest County Government Office as the manager of the Adult Education Data System and by the Central Statistical Office on the basis of the law. It may provide access to

the information on its adult education activities and the training programme to clients, training participants and the Minister responsible for adult education (§ 17 of the Fktv).

V. DATA SECURITY

The Data Controller undertakes to ensure the security of the data, to take measures to ensure that the data recorded, stored or processed are protected and to take all necessary measures to prevent their destruction, unauthorised use or unauthorised alteration.

It also undertakes to require any third party to whom it may transfer or disclose the data to comply with its obligations in this regard.

No automated decision-making or profiling is carried out on the basis of your personal data.

The Data Controller shall take all security, technical and organisational measures to ensure the security of the data.

V.1. Organisational measures

The Data Controller allows access to its IT systems to an individual with rights that can be linked to them. The allocation of access is based on the principle of "necessary and sufficient rights", i.e. each user may use the Data Controller's IT systems and services only to the extent necessary for the performance of their task, with the corresponding rights and for the necessary duration. Access rights to IT systems and services may be granted only to persons who are not restricted for security or other reasons (e.g. conflict of interest) and who have the necessary professional, business and information security skills to use them safely.

V.2. Technical measures

The Data Controller protects its internal network with multiple layers of firewall protection. At all access points to the public networks used, a hardware firewall (border protection device) is installed at all times. Data is stored redundantly, i.e. in multiple locations, by the Data Controller to protect it from destruction, loss, damage or unlawful destruction due to IT equipment failure. We protect our internal networks from external attacks with multi-layered, active, complex malware protection (e.g. virus protection). The necessary external access to the IT systems and databases operated by the Data Controller is provided by the Data Controller via an encrypted data connection (VPN) and the Data Controller's websites are SSL certified. We do our utmost to ensure that our IT tools and software are always up-to-date and in line with the technological solutions generally accepted in the market. We are developing systems that use logging to control and monitor operations and detect incidents such as unauthorised access. The Data Controller's server is located on a separate dedicated server of the hosting provider, protected and locked.

VI. OTHER PROVISIONS

VI.1. The adult education state administration body shall keep an electronic record of the data and the certificate issued by the adult educator for the purpose of the control pursuant to § (1) of Article 20 of the Fktv. and the operation of the career tracking system, and shall manage the data in the record until the last day of the fiftieth year from the date of their creation. The adult education state administration body shall keep the data of the central register containing the

certificates until the last day of the fiftieth year after their creation, after which it shall transfer them to the competent archives and delete the transferred data.

VI.2. Only the Data Controller has access to personal data processed in connection with the provision of adult education. In the event that proceedings are brought before a court or other authority requiring the transmission of personal data to the court or authority, the court or authority may also have access to the personal data.

VI.3 In all cases where the Data Controller intends to use the data provided for a purpose other than that for which it was originally collected, the Data Controller shall inform you thereof and obtain your prior explicit consent or provide you with the opportunity to prohibit such use.

VI.4. The Data Controller reserves the right to unilaterally change this Policy at any time. In the event of any modification of this Notice, the Data Controller shall notify the data subjects thereof.

VI.5. The Notice is available in electronic form on the website of the Data Controller (www.mdakft.hu) and in paper form at its registered office.

Annex

Details of data subjects' rights and remedies in relation to data processing

Knowing the rights and remedies of the data subject (hereinafter referred to as the data subject) in relation to data processing is important because the data controller processes personal data. Personal data is any information by which the data subject can be identified. Thus, personal data is not only the name or identification mark of the data subject, but also knowledge their physical, mental, etc. identity.

The data subject may exercise their rights in relation to data management by contacting the data controller, who shall inform the data subject of the action taken on the request without undue delay and at the latest within one month of receipt of the request. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The data controller shall inform the data subject of the extension, stating the reasons for the delay, within one month of receipt of the request. Where the data subject has made the request by electronic means, the information shall, if possible, be provided by electronic means, unless the data subject requests otherwise.

Below is an explanation of some of the rights of the data subject.

1. Right to transparent information (Articles 12-14 GDPR)

The data controller hereby fulfils its obligation to inform the data controller, the data protection officer, the purposes and legal basis of the processing, the duration of the processing, the data subject's rights and remedies and, where the data do not originate from the data subject, the source of the data. Verbal information may be provided at the request of the data subject, provided that they prove their identity.

2. Right of access of the data subject (Article 15 GDPR)

The data subject may request from the data controller access to personal data relating to them, including a copy of the personal data which are the subject of the processing. The data subject shall have the right to obtain from the data controller feedback as to whether or not their personal data are being processed and, if such processing is ongoing, the right to access the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of recipients to whom or with whom the personal data have been or will be disclosed, including in particular recipients in third countries or international organisations;

- d) where applicable, the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period;
- e) the right of the data subject to obtain from the data controller the rectification, erasure or restriction of the processing of personal data concerning them and to object to the processing of such personal data;
- f) the right to lodge a complaint with a supervisory authority;
- g) if the data were not collected from the data subject, any available information on their source;
- h) the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

3. Right to rectification (Article 16 GDPR)

The data subject shall have the right to obtain, at their request and without undue delay, the rectification by the data controller of inaccurate personal data relating to them. Having regard to the purposes of the processing, the data subject shall have the right to obtain the rectification of incomplete personal data, including by means of a supplementary declaration.

4. Right to erasure: "the right to be forgotten" (Article 17 GDPR)

Personal data must be deleted if

1. the purpose of the processing has ceased;
2. the data subject has withdrawn their consent and there is no other legal basis for the processing;
3. the processing is based on a legitimate interest or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and the data subject objects to the processing;
4. the processing is unlawful;
5. the personal data must be erased in order to comply with a legal obligation under EU or Member State law to which the data controller is subject;
6. data were collected on information society services offered directly to children.

5. Right to restriction of processing (Article 18 GDPR)

The data controller shall restrict processing at the request of the data subject where

1. the data subject contests the accuracy of the personal data;
2. the processing is unlawful and the data subject opposes the erasure of the data;
3. the data controller no longer needs the personal data but the data subject requires them for the establishment, exercise or defence of legal claims;

4. the processing is based on a legitimate interest or is necessary for the performance of a task carried out in the public interest/ in the exercise of official authority vested in the data controller, and the data subject objects to the processing.

6. Obligation to notify the rectification or erasure of personal data or restriction of processing (Article 19 GDPR)

The data controller shall inform any recipient to whom or with which the personal data have been disclosed of the rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. The data subject shall, upon request, be informed by the data controller of those recipients.

7. Right to data portability (Article 20 GDPR)

The data subject shall have the right to obtain the personal data concerning them which they have provided to a data controller in a structured, commonly used, machine-readable format and the right to transmit those data to another data controller without hindrance from the data controller to whom the personal data have been provided, where the processing is based on consent or a contract and the processing is automated. In exercising the right to data portability, the data subject shall have the right to request, where technically feasible, the direct transfer of personal data between data controllers. The exercise of this right shall be without prejudice to the right to be forgotten.

8. Right to object (Article 21 GDPR)

The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data on grounds of legitimate interest or if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, including profiling based on those legal grounds. In such a case, the data controller may no longer process the personal data unless the data controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

9. Right of the data subject in case of automated decision-making (Article 22 GDPR)

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

This provision does not apply in the following cases:

- a) necessary for the conclusion or performance of a contract between the data subject and the data controller;
- b) is permitted by EU or Member State law applicable to the data controller which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or
- c) is based on the explicit consent of the data subject.

The data controller shall ensure that the data subject has at least the right to obtain human intervention by the data controller, to express their views and to object to the decision.

10. Recourse to legal remedies: options available in general

10.1. Data Protection Officer (Articles 38-39 GDPR)

Data subjects can contact the Data Protection Officer for all matters relating to the processing of their personal data and the exercise of their rights under the GDPR (Article 38(4) GDPR). If the data controller fails to act on a request from the data subject, the data controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with a supervisory authority and to seek judicial remedy (Article 12(4) GDPR).

10.2. Procedures that may be initiated at the National Authority for Data Protection and Freedom of Information (Articles 57-58, 77, Infotv. 7 51/A (1), § 52-54, § 55 (1)-(2), § 56-58, § 60-61 GDPR)

Anyone (i.e. not only the data subject) may lodge a complaint with the National Authority for Data Protection and Freedom of Information (hereinafter the Authority), in order to initiate an investigation on the grounds that a personal data breach has occurred or is imminent. It is important that the notification is not anonymous, otherwise the Authority may reject the notification without any substantive investigation. Further grounds for refusal are set out in the Infotv. § 53.

The Authority's investigation is free of charge and the costs of the investigation are advanced and borne by the Authority. Detailed rules on the conduct of the procedure are laid down in the Infotv. § 54, § 55(1)-(2), § 56-58.

In order to enforce the right to the protection of personal data, the Authority shall, upon request of the data subject, initiate a data protection authority procedure pursuant to § 60-61 of the Infotv.

10.3. Enforcement before the courts (Article 79 GDPR, § 23 Infotv.)

The data subject may take the data controller to court if their rights are infringed, as all data subjects have an effective judicial remedy if they consider that their rights under the GDPR have been infringed as a result of the processing of their personal data in a way that does not comply with the GDPR (see above).

The action against the data controller or processor must be brought before the courts of the Member State in which the data controller or processor is established. Such proceedings may also be brought before the courts of the Member State in which the data subject has their habitual residence, unless the data controller or processor is a public authority of a Member State acting in its exercise of official authority.

In Hungary, one can also bring the case before the court of their domicile or residence, at their choice.

The data subject may claim damages/fees from the data controller in the action: - if the data controller causes damage to another person by unlawful processing of the data subject's data or by breaching the requirements of data security, the data subject shall compensate the damage; - if the data controller infringes the data subject's right to privacy by unlawful processing of the data subject's data or by breaching the requirements of data security (e.g. by disclosing or communicating personal data to an unauthorised person), the data subject may claim damages from the data controller.