Gourmand Alapítvány
Belső adatkezelési és adatbiztonsági szabályzat

I. A szabályzat hatálya

1. Jelen szabályzat hatálya kiterjed a Gourmand Kereskedelmi , Vendéglátóipari , Idegenfogalmi Szakképzési Alapítvány egészére, valamennyi szervezeti egységére és az összes foglalkoztatottjára (a továbbiakban: Szervezet).

II. A szabályzat célja

2. A Szabályzat célja, hogy biztosítsa a személyes adatok alaptörvény szerinti védelmének érvényesülését, az információs önrendelkezés megvalósulását, továbbá, hogy a Szervezet által kezelt személyes adatok tekintetében meghatározza az adatkezelés során irányadó adatvédelmi és adatbiztonsági szabályokat.

III. Irányadó jogszabályok

3. A Szervezetnek az adatkezelése során az alábbi jogszabályokban foglalt előírásoknak megfelelően kell eljárnia, a jelen belső szabályzatban foglaltak szerint:

   - Az Európai Parlament és a Tanács (Eu) 2016/679 Rendelete (2016. április 27.) 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, a továbbiakban: GDPR)
   - az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)
   - a polgári törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.)
   - a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.)
   - az elektronikus és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. tv. (Eügyintézési tv)

IV. Értelmező rendelkezések

4. A GDPR-ban meghatározott fogalmak, amelyek közül jelen belső szabályzat jellegével összhangban az alábbi fogalmak emelendők ki :

   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) adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

   c) adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit

önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

d) adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

e) címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

f) 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.

g) nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

h) 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.

i) adatvagyon leltár: az adatkezelő által kezelt személyes adatok körének és jellegének felmérését szolgáló dokumentum.

j) technikai és szervezési intézkedések: az adatkezelő által az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelően meghatározott eljárásrend annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

V. Az adatkezelés alapelvei

5. A Szervezet az adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi (jogszerűség, tisztességes eljárás és átláthatóság).

6. A Szervezet a személyes adatok gyűjtését csak meghatározott, egyértelmű és jogszerű célból végzi, és azokat nem kezeli ezekkel a célokkal össze nem egyeztethető módon (célhoz kötöttség).

7. A Szervezet az adatkezelést annak célja(i) szempontjából megfelelően és relevánsan, és a szükségesre korlátozva végzi (adattakarékosság). Ennek megfelelően a Szervezet nem gyűjt és nem tárol több adatot, mint amennyi az adatkezelés céljának a megvalósulásához feltétlenül szükséges.

8. A Szervezet adatkezelése pontos és naprakész. A Szervezet minden észszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan adatokat haladéktalanul törlésre vagy helyesbítésre kerüljenek (pontosság).

9. A Szervezet a személyes adatokat az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, figyelemmel a vonatkozó jogszabályokban meghatározott tárolási kötelezettségre (korlátozott tárolhatóság).

10. A Szervezet megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, ideértve a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet (integritás és bizalmas jelleg).

11. A Szervzet felelős a fentiekben részletezett alapelveknek való megfelelésért, Ennek értelmében a Szervezet gondoskodik a jelen belső szabályzatban foglaltak folyamatos érvényesüléséről, az adatkezelésének felülvizsgálatáról és szükség esetén az módosításáról, kiegészítéséről.

VI. Adatkezelési jogalapok

12. A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább a 13-18. pontban meghatározott jogalapok egyike teljesül:

13. Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez (a továbbiakban: hozzájáruláson alapuló adatkezelés).

14. Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (a továbbiakban: szerződésen alapuló adatkezelés).

15. Az adatkezelés a Szervezet vonatkozó jogi kötelezettség teljesítéséhez szükséges (a továbbiakban: jogi kötelezettségen alapuló adatkezelés).

16. Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (a továbbiakban: létfontosságú érdeken alapuló adatkezelés).

17. Az adatkezelés közérdekű vagy a Szervezet ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (a továbbiakban: közhatalmi jogosítványon alapuló adatkezelés).

18. Az adatkezelés a Szervezet vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek (a továbbiakban: jogos érdeken alapuló adatkezelés).

19. A Szervezet egy adott személyes adatkör kezelése vonatkozásában mindig csak egy jogalap alapján végzi az adatkezelést. Az adatkezelés jogalapja az adatkezelés során változhat.

VII. Az adatvagyon leltár

20. A Szervezet a tevékenysége körében végzett adatkezelésre vonatkozó, a GDPR és a jogszabályok által előírt kötelezettségeknek megfelelő technikai és szervezési intézkedések megalkotása céljából adatvagyon leltárt készít. Az adatvagyon leltár t artalmazza a Szervezet által kezelt összes adatkört.

21. A Szervezet adatkezelési tevékenységével összefüggésben az adatvagyon leltárban meghatározásra kerülnek az alábbiak:

    a) az érintett az adatkezelés megnevezése és célja
    b) a kezelt adatok köre
    c) esetlegesen kezelt különleges adatok köre
    d) az adatkezelés jogalapja
    e) az adatkezelés időtartama
    f) kik férhetnek hozzá a személyes adatokhoz a vállalkozás szervezetén belül
    g) ki számára kerülhet az adat továbbításra
    h) alkalmaz-e a vállalkozás adatfeldolgozót, ha igen kit, milyen célra és milyen személyes adatokhoz férhet hozzá és mennyi ideig tárolhatja a személyes adatokat

22. A Szervezet adatfeldolgozási tevékenységével összefüggésben (amennyiben van ilyen) az adatvagyon leltárban meghatározásra kerülnek az alábbiak:

    a) mely tevékenységéhez kötötten minősül a Szervezet adatfeldolgozónak;
    b) ki az adatkezelő, akinek a nevében végzi az adatfeldolgozási tevékenységet ;
    c) milyen személyes adatokhoz fér hozzá;
    d) mennyi ideig tárolhatja a személyes adatokat.

VIII. Az érintett jogai és azok érvényesítése

23. A Szervezet a GDPR rendelkezéseivel összhangban az alábbiakat biztosítja az érintettek számára.

    Tájékoztatáshoz való jog

24. A tájékoztatáshoz való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

25. A Szervezet tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújt tájékoztatást az érintettek számára.

26. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni.

Tájékoztatás az érintett kérésére

27. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

28. A Szervezet indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 30 napon belül tájékoztatja az érintettet az egyéb érintetti jogokra vonatkozó érintetti kérelem nyomán hozott intézkedésekről.

29. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, a 30 napos határidő további 60 nappal meghosszabbítható. A határidő meghosszabbításáról a Szervezet a késedelem okainak megjelölésével a kérelem kézhezvételétől számított 30 napon 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.

30. A tájékoztatást és intézkedést díjmentesen kell biztosítani.

31. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, úgy a Szervezet , figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:
    a) észszerű összegű díjat számíthat fel, vagy
    b) megtagadhatja a kérelem alapján történő intézkedést.

32. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a Szervezetet terheli.

Kötelező tájékoztatás

33. Amennyiben a Szervezet az adatokat közvetlenül az érintettől szerezte meg, úgy a Szervezet mindenképpen tájékoztatást nyújt az alábbiakról:

    a) a Szervezet képviselőjének a kiléte és elérhetőségei;
    b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
    c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja
    d) a jogos érdeken alapuló adatkezelés esetén, a Szervezet vagy harmadik fél jogos érdekei;
    e) adott esetben a személyes adatok címzettjei

34. A személyes adatok első megszerzésének időpontjában a Szervezet a fentieken túl az érintetteket tájékoztatja az alábbiakról is:

a) a személyes adatok tárolásának időtartamáról
b) az érintett azon jogáról, hogy kérelmezheti a Szervezet a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, egyes jogalapokhoz tartozó adatkezelés esetében törlését vagy kezelésének korlátozását, és egyes jogalapokhoz tartozó adatkezelés esetében tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
c) a hozzájáruláson alapuló adatkezelés bármely időpontban történő visszavonásához való jogról, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
d) a felügyeleti hatósághoz (Nemzeti Adatvédelmi Hatóság, továbbiakban: Hatóság vagy NAIH) címzett panasz benyújtásának jogáról;
e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.

35. Ha a Szervezet a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és a 34. pontban említett minden releváns kiegészítő információról.

36. A Szervezet a kötelező tájékoztatásnak többféle módon tehet eleget.

a) A 34. pontban foglalt információkat a Szervezet ("Adatkezelési tájékoztató" címen) közzéteszi a honlapján olyan módon, hogy az könnyen megtalálható és könnyen elérhető legyen bárki számára.

b) A honlapon való közzététel mellett vagy helyett, a Szervezet választhatja az "Adatkezelési tájékoztató" szerződés mellékleteként történő hozzáférhetővé tételét. Ebben az esetben elegendő az adott érintetti körre vonatkozó adatkezelési tájékoztatást az érintett rendelkezésére bocsátani.

Hozzáférés joga

37. A hozzáférés joga minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

38. Az érintett jogosult arra, hogy a Szervezettől 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 a Szervezet közölte vagy közölni fogja
d) adott esetben a személyes adatok tárolásának tervezett időtartama
e) az érintett azon joga, hogy kérelmezheti a Szervezettől a rá vonatkozó személyes adatok helyesbítését, egyes jogalapokhoz kötött adatkezelés esetén

ezen adatok törlését vagy kezelésének korlátozását, és egyes jogalapokhoz kötött adatkezelés esetén tiltakozhat az ilyen személyes adatok kezelése ellen;

f) a felügyeleti hatósághoz címzett panasz benyújtásának joga;

g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

39. A Szervezet az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsáthatja.

40. Az érintett által kért további másolatokért a Szervezet az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, melynek mértékét a vállalkozás árszabási szabályzata, egyéb szabályzata, vagy egyéb dokumentum tartalmazza.

Helyesbítéshez való jog

41. A helyesbítéshez való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

42. A Szervezet az érintett erre irányuló kérelme esetén indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozóan pontatlanul kezelt személyes adatokat. Az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Töréshez (elfeledtetéshez) való jog

43. A törléshez (elfeledtetéshez) való jog nem illeti meg az érintettet automatikusan, minden jogalaphoz kapcsolódó adatkezelés vonatkozásában.

44. A Szervezet indokolatlan késedelem nélkül törli az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását (hozzájáruláson alapuló adatkezelés esetén), és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre

d) a személyes adatok jogellenesen kerültek kezelésre;

e) a személyes adatokat a Szervezetre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

45. Az érintett törlési kérelmének a Szervezet nem tesz eleget, amennyiben az adatkezelés szükséges a személyes adatok kezelését előíró, a Szervezetre alkalmazandó jogszabályi kötelezettség teljesítéséhez.

46. Amennyiben a Szervezethez törlési kérelem érkezik, a Szervezet első lépésként megvizsgálja, hogy a törlési kérelem valóban a jogosulttól származik-e. Ennek érdekében a Szervezet elkérheti az érintett és a Szervezet között fennálló szerződés azonosítására szolgáló adatokat (például szerződésszám, szerződés kelte), az érintett

számára a Szervzet által kiállított irat azonosító számát, az érintettről nyilvántartott személyazonosító adatok megadását (a Szervezet azonban nem kérhet azonosításként olyan plusz adatot, amelyet az érintettről nem tart nyilván).

47. Amennyiben a Szervezetnek eleget kell tennie a törlési kérelemnek, úgy köteles mindent megtenni annak érdekében, hogy a személyes adat az összes adatbázisból törlésre kerüljön.

Az adatkezelés korlátozáshoz való jog

48. A korlátozáshoz való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

49. A Szervezet az érintett kérésére korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:
    a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a Szervezet ellenőrizze a személyes adatokat ;
    b) az adatkezelés jogellenes és az érintett ellenzi az adatok törlését és ehelyett kéri azok felhasználásának korlátozását;
    c) a Szervezetnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez.

50. Ha az adatkezelés az előző pont alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

51. A Szervezet tájékoztatja a kötelezettségről mindazokat, akik számára a személyes adat továbbításra került.

Tiltakozás

52. A tiltakozás joga az érintettet a közhatalmi jogosítványon alapuló vagy jogos érdeken alapuló adatkezelési jogalapok esetében illeti meg.

53. A Szervezet az érintett tiltakozás iránti kérelme esetén a személyes adatokat nem kezelheti tovább, kivéve, ha 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.

54. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen.

55. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Adathordozhatósághoz való jog

56. Az adathordozhatósághoz való jog a hozzájáruláson vagy a szerződésen alapuló adatkezelési jogalap esetében illeti meg az érintettet, ha az adatkezelés automatizált módon történik.

57. A Szervezet biztosítja, hogy érintett a rá vonatkozó, általa a Szervezet számára rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, olvasható formátumban megkapja.

IX. Adatkezelési tevékenységek nyilvántartása

58. Az adatkezelési tevékenységek nyilvántartását a Szervezet az elszámoltathatóság elvéből következően annak érdekében végzi, hogy az GDPR-nak való megfelelést nyomon tudja követni, és igazolni tudja.

59. A Szervezet a felelősségébe tartozóan végzett adatkezelési tevékenységekről legalább az alábbi nyilvántartásokat vezeti:

    a) adattovábbítás nyilvántartása
    b) érintetti jogok érvényesítése iránti kérelmek és az arra a Szervezet által adott válaszok nyilvántartása
    c) hatósági megkeresések és az arra a Szervezet által adott válaszok nyilvántartása
    d) adatkezelés megszüntetése iránti kérelmek nyilvántartása
    e) ügyfelek nyilvántartása
    f) marketing célú megkeresések nyilvántartása
    g) munkaviszonnyal összefüggő személyes adatok kezelésének nyilvántartása
    h) munkaerő-felvétel nyilvántartása
    i) adatvédelmi incidensek nyilvántartása.

60. A Szervezt a felelősségébe tartozóan végzett, a 59. pontban meghatározott adatkezelési tevékenységekről vezetett nyilvántartásait az alábbi tartalommal vezeti:

    a) a Szervezt neve és elérhetősége, valamint – ha van ilyen – a Szervezet képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
    b) az adatkezelés céljai;
    c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
    d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják
    e) adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk;
    f) a különböző adatkategóriák törlésére előirányzott határidők;
    g) a technikai és szervezési intézkedések általános leírása.

61. A nyilvántartásokat a Szervezt írásban vezeti, papír alapon vagy elektronikus formátumban.

X. Adatbiztonsági rendelkezések

62. A Szervezt 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 megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

63. Előzőek értelmében a Szervezet köteles garantálni az általa kezelt adatok bizalmasságát, sérthetetlenségét és rendelkezésre állását.

64. Az adatkezelés biztonsága megvalósítása érdekében a Szervezet fizikai, logikai és adminisztratív kontrollokat alkalmaz együttesen.

65. A Szervezet legalább az alábbi fizikai kontrollokat alkalmazza:

a) a Szervezet a jogosulatlan személyek belépésének kiszűrésére alkalmas beléptetési rendszer működtetésével biztosítja, hogy épületébe/irodájába jogosulatlan személyek ne léphessenek be
b) a Szervezt az általa mind elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy

66. A Szervezet legalább az alábbi logikai kontrollokat alkalmazza:
A Szervezet biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá

67. A Szervezt legalább az alábbi adminisztratív kontrollokat alkalmazza:

a Szervezet biztosítja olyan iratkezelési eljárásrend kialakítását, hogy a hozzá tévesen beérkező személyes adatokat tartalmazó iratok a lehető leghamarabb kiszűrésre kerüljenek és azokat csak a lehető legszűkebb személyi kör ismerje.

XI. Adatvédelmi incidensek kezelése

68. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

69. Az adatvédelmi incidenst a Szervezt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a hatóságnak.

70. Az adatvédelmi incidenst nem kell a hatóságnak bejelenteni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

71. Amennyiben a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

72. Amennyiben az adatvédelmi incidens hatóság számára történő bejelentése szükséges, úgy a bejelentésben:

    a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
    b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
    c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
    d) ismertetni kell a Szervezet által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

73. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Szervezet indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

74. A 73. pont szerinti tájékoztatásban az érintettel világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell:

    a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
    b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
    c) ismertetni kell a Szervezet által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

75. Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

    a) a Szervezet megfelelő technikai és szervezési -védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
    b) a Szervezet az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

76. Amennyiben a Szervezet adatfeldolgozót alkalmaz, úgy az adatfeldolgozó szerződésben ki kell kötni, hogy az adatfeldolgozó köteles a nála bekövetkezett adatvédelmi incidenst haladéktalanul bejelenteni a vállalkozásnak.

XII. Munkaviszonnyal összefüggő adatkezelések

77. A Szervezt a 36. pont szerinti "Adatkezelési tájékoztatóba" belefoglalja az álláspályázatokra vonatkozóan a 33. és 34. pontban meghatározottakat. A Szervezet az általa kiírt álláspályázatban az elérhetőség megjelölésével hivatkozik az "Adatkezelési tájékoztatóra". Amennyiben a Szervezet nem elektronikus úton tette elérhetővé az "Adatkezelési tájékoztatót", úgy a vonatkozó rendelkezéseket az álláspályázatba foglalja.

78. Amennyiben a Szervezet az állás betöltését követően is tárolni kívánja az álláspályázó által beadott iratokat, úgy ehhez az álláspályázó hozzájárulását kell kérni. A hozzájárulásnak önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Ennek érdekben a hozzájáruló nyilatkozatnak legalább az alábbiakat kell tartalmaznia:

a) a Szervezet képviselőjének kiléte és elérhetőségei;
b) a személyes adatok tervezett kezelésének célja valamint az adatkezelés jogalapja (hozzájáruláson alapuló);
c) a személyes adatok tárolásának időtartama;
d) az érintett azon joga, hogy kérelmezheti a Szervezettől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását;
e) az érintett azon joga, hogy bármely időpontban visszavonhatja a hozzájárulását, amely azonban nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
f) a hatósághoz címzett panasz benyújtásának jogáról.

79. A pályázat elbírálása után az eredménytelen pályázók személyes adatait tartalmazó adathordozókat a pályázónak a személyes adatai további pályázatok során történő felhasználására vonatkozó hozzájárulása hiányában meg kell semmisíteni.

80. A Szervezt a munkavállalók adatait a Mt. vonatkozó rendelkezései alapján kezeli és az Mt-ben meghatározott módon tájékoztatja, a GDPR-ban foglalt adatkezelési alapelvek betartása mellett.

81. A Szervezet a munkavállalóknak tájékoztatást ad az általa igénybe vett adatfeldolgozókkal kapcsolatban azok kilétéről és a számukra továbbított adatok köréről.

82. A munkaviszonyban történő adatkezelés során jellemzően az alábbi jogalapok merülhetnek fel:

a) szerződésen alapuló
b) jogi kötelezettségen alapuló
c) jogos érdeken alapuló

XIII. Az adatfeldolgozó igénybevételére vonatkozó rendelkezések

83. Ha az adatkezelést a Szervezet nevében más végzi a Szervezet kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

84. Az adatfeldolgozó a Szervezet előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

85. Az adatfeldolgozó által végzett adatkezelés vonatkozásában a Szervezet és az adatfeldolgozó szerződést kötnek. Ezen szerződés az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint a Szervezet kötelezettségeit és jogait határozza meg.

86. Az előző pont szerinti szerződés különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag a Szervezet utasításai alapján kezeli,
b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
c) alkalmazza a legalább a Szervezet által előírt szintű adatbiztonsági intézkedéseket;
d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan fentebb említett feltételeket;
e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a segíti a Szervezetet abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
f) segíti a Szervezetet az adatvédelmi incidens szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
g) vállalja, hogy a nála bekövetkező adatvédelmi incidens esetén haladéktalanul tájékoztatja erről a Szervezetet ;
h) az adatkezelési szolgáltatás nyújtásának befejezését követően a Szervezet döntése alapján minden személyes adatot töröl vagy visszajuttat a Szervezetnek és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő.

87. Az adatfeldolgozó és a nála személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag a Szervezet utasításának megfelelően kezelheti.

XIV. Hatályba léptető és záró rendelkezések

A jelen szabályzat 2018. július 26-én lép hatályba.

Kelt: 2018. július 18.

.....

Hoffmann Rita
kuratórium elnöke

GOURMAND
Kereskedelmi, Vendéglátóipari,
Idegenforgalmi Szakképzési Alapítvány
✉: 1244 Bp., Pf.:843.
Adószám: 18049828-1-41