Adatvédelmi és adatkezelési szabályzat

3.0 verzió

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint 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) AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE alapján –

Hatályos 2024. szeptember 1. napjától

Concerto Akadémia Nonprofit Kft.
1094 Budapest, Páva utca 10-12.
Tel.: +36 1 215 5770, fax: +36 1 215 5462
www.concertobudapest.hu

Tartalomjegyzék

1. A Szabályzat célja

A jelen Szabályzat a Concerto Akadémia Nonprofit Korlátolt Felelősségű Társaság (székhely: 1094 Budapest, Páva u. 10-12., Cg.: 01-09-177086, adószám: 18312777-2-43, nyilvántartó cégbíróság: Fővárosi Törvényszék Cégbírósága, Telefonszám: +36 1 215 5770, e-mail cím: jegy@concertobudapest.hu, info@concertobudapest.hu, fax szám: +36 1 215 5462, levelezési cím: 1450 Budapest, Pf. 75.) (továbbiakban Concerto) mint adatkezelő által alkalmazott adatvédelmi és adatkezelési elveket és eljárásokat rögzíti.

A jelen Szabályzat célja, hogy a Szervezet az általa nyújtott valamennyi szolgáltatás során biztosítsa az Ügyfél számára a személyes adatainak az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 rendelete, valamint az adatvédelmi törvényben (Infotv.), valamint jelen Szabályzatban meghatározott elvek szerinti tisztességes, kiszámítható és jogszerű adatkezelését a következők szerint:

- meghatározza a *Szervezet* által kezelt adatok körét, az adatkezelési folyamatok céljait és az egyes céloknak megfelelően rendelje a célokhoz az adatkezelés jogalapját és az egyes adatok kezelésének időkorlátait. Megbízhatóan alapja legyen a természetes személyek tájékoztató anyagainak, illetve biztosítsa a természetes személyek jogait a róluk tárolt adatok tekintetében,
- biztosítsa a *Szervezet* tevékenysége során a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését,
- a *Szervezet* által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza az adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat,
- a *Szervezet* feladatai teljesítéséhez, valamint a nyilvántartások vezetéséhez kapcsolódóan meghatározza a *Szervezet a* nyilvántartások vezetésének rendjét,
- meghatározza a *Szervezet* adatszolgáltatási rendjét,
- biztosítsa az Uniós adatvédelmi rendelet (GDPR), valamint a tagállami jogi szabályozás, így az alaptörvényben, Infotv.-ben meghatározott Érintetti, Adatkezelői, Adatfeldolgozói, Címzetti jogokat és kötelezettségeket.

2. Általános szabályok

2.1. A szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed a Szervezettel jogviszonyban álló minden munkavállalóra, munkavégzésre irányuló jogviszonyban álló természetes személyre, valamint a Szervezet megbízásából, szerződés alapján, adatfeldolgozói feladatokat ellátó partnerére.

2.2. A szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed a *Szervezet*nél folytatott valamennyi papíralapú és elektronikus adatkezelésre.

2.3. A szabályzat időbeli hatálya

A hatályosság visszavonásig, illetve módosításig érvényes. Az Adatkezelőnek joga és kötelezettsége a szabályzat rendszeres felülvizsgálata és a jogszabályi környezet változásainak szabályzaton belüli átvezetése. Ezt a feladatot a szabályzat verzió számmal történő módosításával igazolja. A módosításokat oly módon köteles átvezetni, hogy a szabályzat módosulását követnie kell a tájékoztató anyagok naprakészségének és a változások hatályba léptetését megelőzően legalább 15 nappal közzé kell tennie a megváltozó tájékoztatót és felhívni az érintettek figyelmét a változások hatálybalépésének dátumára.

2.4. Kapcsolódó szabályzatok, eljárások, rendelkezések

Kamera kezelési szabályzatok
Incidenskezelési szabályzat
Adatkezelési tájékoztató
Adatkezelési nyilatkozat (munkavállaló)
Adatfeldolgozói megállapodás (adatfeldolgozó és alvállalkozó)
Kockázatelemzés
Adatvédelmi incidens nyilvántartás
Érintetti igény nyilvántartás
Incidens nyilvántartás
Adatkezelési folyamatok nyilvántartása
Közérdekű adatigénylés nyilvántartása
Érdekmérlegelési tesztek

2.5. Értelmező fogalommeghatározások

„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;
„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;

„az adatkezelés korlátozása": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

„profilalkotás": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;

„álnevesítés": a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

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

„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;

„adatfeldolgozó": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

„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;

„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;

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

„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;

„genetikai adat": egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

„biometrikus adat": egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;
„egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;
„képviselő": az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy, aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;
„vállalkozás": gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is;
„vállalkozáscsoport": az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;
„kötelező erejű vállalati szabályok": a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;
„felügyeleti hatóság": egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv;
„érintett felügyeleti hatóság": az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;
b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy
c) panaszt nyújtottak be az említett felügyeleti hatósághoz.

3. Az adatkezelés jogszerűségéhez kapcsolódó szabályok

3.1. Általános elvek

A *Szervezet* adattárolása olyan formában történik, amely az Érintettek azonosítását a személyes adatok kezelése céljainak a célokhoz rendelt jogalapoknak megfelelő és szükséges idő figyelembevételét lehetővé teszi, és biztosítja az alábbi elvek megvalósulását.
Ugyanakkor a tárolt és kezelt adatok szempontjából mindent meg kell tenni az adatok védelmében adatkezelőként. Az adatkezelés során igénybe vett Adatfeldolgozókkal szemben érvényesíteni kell azokat az elveket és elvárásokat, amelyek tekintetében az adatok sérülésének kockázata minimalizálható.

3.2. A személyes adatok különleges kategóriáinak kezelése

A Szervezet, mint adatkezelő, nem végez a személyes adatok tekintetében semmilyen különleges kategóriába tartozó adatkezelést. Azaz, sem faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, vagy szakszervezeti tagságra utaló személyes adatot, biometrikus, vagy egészségügyi adatot, a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatokat nem tart nyilván és nem rögzít.

3.3. Elszámoltathatóság

A Szervezet, mint Adatkezelő a felelős a GDPR 5. cikk 1. bekezdésben meghatározott elvek megvalósulásáért. Mint Adatkezelőnek, képesnek kell lennie a megfelelés igazolására.

3.4. Jogszerűség, tisztességes eljárás és átláthatóság

A személyes adatok kezelését jogszerűen és tisztességesen, valamint az Érintettek számára átláthatóan kell végezni, biztosítva az Érintetti jogok gyakorlásának zökkenőmentes megvalósulását.

3.5. Célhoz kötöttség

A Szervezet a személyes adatok gyűjtése tekintetében csak meghatározott, egyértelmű és jogszerű céllal tárol adatokat, és nem kezel adatokat a célokkal nem összeegyeztethető módon.

3.6. Adattakarékosság

A tárolt adatoknak az adatkezelés céljai szempontjából relevánsnak és megfelelőnek kell lennie, és a szükséges adatokra kell korlátozódnia. Ugyanakkor folyamatosan igazodnia kell a változó technológiai és jogi szabályozási környezethez. A változásokról az Érintetteket a változás mértékének, kockázatának megfelelő módon tájékoztatókon vagy személyes megkeresés útján kell tájékoztatnia.

3.7. Pontosság

Az észszerűség határain belül pontosnak, naprakésznek kell lenni. A szervezet által tárolt és kezelt adatok tekintetében, az adatmódosítási kérelmeket a jogszabályi környezetnek megfelelően kell kezelni. A nyilvántartások vezetése során a saját rögzítésű adatokat az adatváltozás bejelentők alapján kell módosítani, ugyanakkor az átadás átvétel keretében átvett adatok tekintetében az adatváltozás bejelentéseket a közhiteles nyilvántartás vezetője felé, a vonatkozó jogszabályoknak megfelelően át kell adni. A pontatlan személyes adatok haladéktalanul törlendők vagy helyesbítendők.

3.8. Korlátozott tárolhatóság

A személyes adattárolásnak olyannak kell lennie, amely az Érinttettek azonosíthatóságát, azonosítását, csak az adatok tárolási céljainak és a célok eléréséhez szükséges ideig teszi lehetővé. Amennyiben az Érintett él adatkorlátozási jogával, a tárolt adatok tekintetében a kezelést fel kell függeszteni és a tárolás fenntartásával párhuzamosan, a korlátozás végéig biztosítani kell azok változatlanságát és sértetlenségét.

3.9. Integritás, bizalmasság

Az Adatkezelő biztosítja a személyes adatok megfelelő biztonságos tárolását és kezelését, ugyanakkor gátolja a jogosulatlan, vagy jogellenes kezelést, a véletlen elvesztést, vagy megsemmisítést.

3.10. Jogalapok

3.10.1. Hozzájárulás

Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. A hozzájárulások beszerzése során teljesülnie kell a következőknek:

3.10.1.1. Önkéntesség

A hallgatás, az előre bejelölt négyzet vagy nem cselekvés nem minősül hozzájárulásnak. Minden hozzájárulásnak amennyiben az nem származtatott hozzájárulás aktív cselekvéssel együt járónak kell lennie.

3.10.1.2. Bizonyítható

Az adatkezelőnek kell bizonyítania a hozzájárulás tényét ezért minden hozzájárulásos adatkezelés esetében az elektronikus felületek logolásából látszani kell, hogy az érintett személy aktívan járult hozzá az adatok kezeléséhez és mindezt mikor tette.

3.10.1.3. Célhoz kötött

Feltételeként csak olyan adat megadását lehet kérni, ami feltétlenül kell a szolgálatatás nyújtásához, vagy a szervezet alaptevékenység ellátásához. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni.

3.10.1.4. Gyermekek és különleges adatok hozzájárulási igénye

A szervezet tevékenységi köréből és az adat kezelések céljait tekintve nem kezel gyermek korúakra vonatkozó személyes adatokat. Amennyiben ez bármely speciális esetkapcsán felmerül, úgy az Uniós rendelet 8.cikk-ben megfogalmazott szabályoknak megfelelően 16. évet be nem töltött gyermekek hozzájárulása csak bizonyítható szülői beleegyezéssel hozzájárulással és annak dokumentálásával kezdhető meg.

3.10.1.5. Közvetlen vagy származtatott hozzájárulás

Közvetlenül az Érintett-től szerezük be az adatokat vagy nem közvetlenül tőle származnak a tárolt adatok az szerint más jellegű tájékoztatást kell biztosítani (13-14. cikk a tájékoztatás eltérése). A szervezet abban az esetben, ha jogos érdekeinek érvényesítése kapcsán nem az Érintettől származó adatokat szerez be, köteles az adatok átadása előtt meggyőződni arról, hogy az adatátadó az Uniós rendeletnek megfelelő forrásból származó adatot szándékozik átadni.

3.10.2. Szerződésen alapuló

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.

3.10.3. Jogi szabályozásra visszavezethető

Az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, az ez alapján tárolt személyes adatok tárolása, kezelése során a jogi környezet változását a szabályozásban követni kell, és szükség esetén a jogalap változásról az érintettet tájékoztatja az adatkezelő.

3.10.4. Az érintett érdekeinek védelme

Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

3.10.5. Közérdekű feladat végrehajtása

Az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges. Kapcsolódik a TILTAKOZÁS JOGA

3.10.6. Adatkezelő vagy harmadik fél jogos érdeke

Az adatkezelés az adatkezelő 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.

Az Adatkezelő a Rendelet 6. cikk (1) bekezdés f) pontja alapján kezelt adatok esetében érdekmérlegelési tesztet végez az alábbiak szerint:

Az érdekmérlegelési teszt során az Adatkezelő:

- azonosítja az érdekmérlegelési teszt tárgyát képező személyes adat kezeléséhez fűződő jogos érdekét,
- megállapítja a Szervezet érdekmérlegelési teszt alapját képező személyes adataival kapcsolatos érdekeit, az érintett érdekeit, mint a Adatkezelő jogos érdekeinek ellenpontját,
- elvégzi jogos érdekeinek és az érintett jogos érdekeinek, alapjogainak vizsgálatát és ez alapján megállapítja, hogy a személyes adat kezelhető-e.
- Kapcsolódó speciális érintetti jog a TILTAKOZÁS JOGA

4. Érintettek jogai

A Szervezet elsőszámú vezetője biztosítja, hogy az Érintett, a Szervezet által kezelt adataival kapcsolatban élhessen az Uniós rendeletben és a tagállami szabályozásban meghatározott jogaival. Az Érintettek jogaikat egyszerűsített, írásban benyújtott kérelem útján érvényesíthetik. Az Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 30 napon belül tájékoztatja az Érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 60 nappal meghosszabbítható. A határidő meghosszabbításáról az Adatkezelő 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.

Az Érintett tájékoztatása, annak kérelme esetén, korlátozások kivételével, kiterjed a kezelt adatok és a forrásának megjelölésére, az adatkezelés céljára, jogalapjára, időtartamára, a

szervezet adatvédelmi felelősének nevére elérhetőségi adataira. Külön kérésre az Adatkezelő tájékoztatja az Adatfeldolgozók és Címzettek adatairól az Érintettet. Az alapvető jogaival az Érintett ingyenesen élhet, de a felmerülő valós és arányos költségek tovább terhelhetők.
Közös Adatkezelő esetében az adatok helyesbítéséről, zárolásáról vagy törléséről mindazokat tájékoztatni kell, akik az adatkezelésben érintettek, valamint azokat a Címzetteket, akiknek az adatot az adatátadási szabályzatnak megfelelően átadja az Adatkezelő.

4.1. Hozzájárulás (visszavonás)

Az érintett hozzájárulását csak és kizárólag egyértelmű cél meghatározása és az önkéntesség bizonyíthatósága esetén kérhet az adatkezelő. Amennyiben bármely Érintett esetében a hozzájárulás jogalapján az Érintett élni kíván a visszavonás vagy ismételt hozzájárulás jogával, az adatkezelőnél írásban jelentheti be szándékát.

4.2. Hozzáférés joga (betekintés)

A Szervezet elsőszámú vezetője biztosítja, hogy az Érintett (aki lehet a Szervezet tagja, tisztségviselője, munkavállalója) a Szervezet által kezelt adataihoz hozzáférjen. A hozzáférést két módon lehet az érintett számára biztosítani.
A Szervezet a kezelt adatokat elektronikus úton hozzáférhetővé teszi, ezt az Adatkezelő helyszínhez és feltételekhez kötheti.
A kezelt adatokat elektronikus formában (elektronikusan hitelesítve) az Érintett rendelkezésére bocsátja, elektronikus tájékoztatás formájában megküldi.
Az elektronikus tájékoztatás ingyenes, ha a tájékoztatást kérő az adott naptári évben azonos adatkezelésre vonatkozó tájékoztatási kérelmet még nem nyújtott be. Minden egyéb esetben a Szervezet a ráfordítással arányos költségtérítést állapíthat meg.

4.3. Helyesbítés joga, és kötelezettsége

Az Érintett tájékoztatást kérhet a Szervezettől a személyes adatainak kezeléséről, és kérheti személyes adatainak helyesbítését.

4.4. Törlés, felejtés joga

Az Érintett kérheti adatainak törlését, felejtését a jogszabályi környezetben meghatározott feltételek fennállásának kötelező adatkezelés előírásait kivéve. A törlés nem jelentheti csak a megjelenés korlátozását, valós fizikai törlést vagy helyreállíthatatlan felülírást jelenthet.
A törlési, felejtési kérelemnek dokumentáltan eleget kell tenni, ha

- az adat kezelése jogellenes,
- az Érintett azt kéri, és az adatkezelés jogalapja a kérésre történt törlést lehetővé teszi
- az adat hiányos vagy téves, és ez az állapot jogszerűen nem orvosolható, feltéve, hogy az adatkezelés jogalapja a kérésre történt törlést lehetővé teszi
- az adatkezelés céljának megfelelő jogalaphoz kapcsolódó határidő lejárt
- azt a bíróság vagy az illetékes hatóság elrendelte.

4.5. Adatkezelés korlátozásának joga

Az Érintett kérheti kezelt adatainak adatkezelési korlátozását a jogszabályi környezetben meghatározott feltételek fennállásának kötelező adatkezelés előírásait kivéve. Ebben az esetben az adatok tárolás továbbra is fennáll, de az adatkezelés nem valósulhat meg.

4.6. Adathordozhatóság joga

Egy példány ingyenes, de az Adatkezelő felmerült költséget felszámolhat.

4.7. Tiltakozás joga

Az Érintett jogainak gyakorlása tekintetében, csak a közérdekű feladat kezelése és az Adatkezelő által jogos érdekké minősített jogalappal rendelkező adatkezelés (továbbítása) ellen élhet tiltakozással.

- A *Szervezet* a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.
- Amennyiben a tiltakozás indokolt, a *Szervezet* köteles az adatkezelést (további adatfelvételt, adattovábbítást) felfüggeszteni és az adatokat zárolni, valamint a tiltakozásról, és az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.
- Ha az Érintett nem ért egyet a tiltakozásának elbírálása eredményeként hozott döntéssel, illetve, ha a *Szervezet* a határidőt elmulasztotta, az Érintett – a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül – érvényes jogi környezetben meghatározott módon bírósághoz fordulhat.

4.8. Érintettek tájékoztatása

Az Érintettet az adatkezelés megkezdése előtt tájékoztatni kell az Infotv. 20.§-ában foglaltak szerint. Ez a tájékoztatás egyénileg írásban, valamint a *Szervezet* honlapján található „adatkezelés" menüpontban elhelyezett tájékoztató formájában is megtehető.

4.9. Érintettek jogorvoslati lehetőségei

Az érintettek jogaik vagy személyes adataik sérülése, vagy vélt sérülése estén fordulhatnak a szervezet adatvédelmi felelőséhez. Amennyiben az érintett az Adatkezelő válasza ellenére jogainak sérülését véli panasszal vagy bejelentéssel élhet a felügyeleti hatóságnál. Az adatkezelő esetleges jogsértése ellen panasszal a Nemzeti Adatvédelmi és Információszabadság Hatóságnál lehet élni:
Nemzeti Adatvédelmi és Információszabadság Hatóság
1055 Budapest, Falk Miksa utca 9-11.
Levelezési cím: 1374 Budapest, Pf. 603.
E-mail: ugyfelszolgalat@naih.hu
A panasztételi jogtól függetlenül az érintett bírósághoz is fordulhat személyes adatai jogellenes kezelése, illetve az információs önrendelkezési jogához kapcsolódó jogai sérelme miatt. Magyarországon a per az érintett lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt, vagy az adatkezelő székhelye alapján illetékes bíróság előtt indítható meg. A lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a https://birosag.hu/birosag-kereso oldalon.

5. Az adatkezelő adatvédelmi szervezete

5.1. Szervezet irányítója és felelőse

A Szervezet adatkezelői tevékenyégének felelős irányítója a Szervezet elsőszámú képviseletre jogosult vezetője vagy az általa megjelölt képviseleti joggal rendelkező felső vezető.

5.2. Külső adatvédelmi tisztviselő

Az Adatkezelő által kiválasztott szakértő, aki a Szervezetben folyó adatvédelmi tevékenység szakmai színvonaláért, a jogszabályi változások átvezetéséért, a tudatosságnövelő tréningek megtartásáért, az incidenskezelésekhez kapcsolódó szakmai irányításért, a kockázatelemzések és hatásvizsgálatok szakmai színvonaláért felel. A válságstáb összehívása esetén irányítja a stáb szakmai munkáját, tartja a kapcsolatot a felügyeleti hatósággal. Tevékenységére a Rendelet által meghatározott jogok és kötelezettségek érvényesek.

5.3. Belső adatvédelmi felelős

Az Adatkezelő munkavállalója, aki a feladatát részmunkaidőben látja el és koordinálja, összefogja az adatvédelmi feladatokat, kellő időben bevonja a külső adatvédelmi tisztviselőt, kezeli, lezárja és nyilvántartja az alacsony kockázati szintű incidenseket. Közepes kockázati szintű incidensek esetén összehívja a munkacsoportot és irányítja annak munkáját. Magas kockázatú incidens esetén összehívja a válságstábot és részt vesz annak munkájában a külső adatvédelmi tisztviselő irányítása alatt.

5.4. Munkacsoport

Változó összetételű közepes kockázatú információbiztonsági és adatvédelmi incidens esetén kerül összehívásra. A belső adatvédelmi felelős hívja össze és irányítja a munkáját. Tagjai a külső adatvédelmi tisztviselő, az informatikai rendszer üzemeltetője, az incidens által érintett szervezeti egység(ek) vezetője, az Érintett adatfeldolgozó kijelölt munkatársa. A munkacsoport tevékenységéről az adatvédelmi szervezet irányítóját folyamatosan tájékoztatni köteles.

5.5. Válságstáb

Változó összetételű magas kockázatú információbiztonsági és adatvédelmi incidens esetén kerül összehívásra. A belső adatvédelmi felelős hívja össze. A munkáját az adatvédelmi szervezet irányítója irányítja a külső adatvédelmi tisztviselővel közösen. Tagjai az adatvédelmi szervezet irányítója, a belső és külső adatvédelmi tisztviselő, az informatikai rendszer üzemeltetője, az incidens által érintett szervezeti egység(ek) vezetője, az Érintett adatfeldolgozó vezető munkatársa.

6. Adatvédelmi felelős és tisztviselő kinevezése és tevékenységének szabályai

A *Szervezetben az* adatvédelmi felelős tekintetében a Szervezet két pozíciót határoz meg. A belső adatvédelmi felelős tevékenységét munkaviszony keretein belül látja el. A külső adatvédelmi tisztviselő a rendeletben meghatározott feladatokat lát el. Az Adatkezelő és a vele szerződéses jogviszonyban álló Adatfeldolgozó is köteles biztosítani, hogy a külső adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon. Az Adatkezelő és az Adatfeldolgozó biztosítja, hogy az adatvédelmi felelős a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el.

6.1. A külső adatvédelmi tisztviselő feladatai

Tájékoztat és szakmai tanácsot ad az Adatkezelő vagy az Adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére. Ellenőrzi az jogszabályi környezetben előírtak megvalósulását és érvényesítését, az adatvédelemmel kapcsolatos szabályok érvényesülését. Munkáját közvetlenül az elsőszámú vezető irányítása mellett végzi. Új adatkezelési folyamatok megkezdése előtt az elsőszámú vezető adatkezelésre vonatkozó döntéseit véleményezi.
Munkája során szakmai iránymutatást ad az Adatkezelő részére, folyamatos támogatást biztosít az adatkezelést végző alkalmazottak részére Európai Parlament és a Tanács (Eu) 2016/679 rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban.
Az Adatkezelő nevében együttműködik a felügyeleti hatósággal. Kapcsolattartóként közreműködik és konzultál a felügyeleti hatósággal az adatkezelést érintő ügyekben.
A kockázatelemzések tekintetében ellátja a szakmai felügyeletet.
A külső adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi. Ellenőrzi a rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést.
Rendszeres felkészítő és ellenőrző munkát végez az adatkezelési műveletekben résztvevő munkavállalók tudatosságnövelése érdekében.
Részt vesz az adatvédelmi auditok előkészítésében, lebonyolításában.
Iránymutatást vállal az informatikai támogatottság és szabályozottság megteremtésében, felülvizsgálatában.
Ellenőrizheti az információ biztonság szabályozottságát, betartását, felülvizsgálatát.
Ellenőrzi a célok, jogalapok és tárolási idők helyes meghatározását, felügyeli a nyilvántartások vezetését. Követi és a megbízó felé továbbítja a jogi környezetben beálló változásokat.
Rendszeresen képzéseket, tudatosságnövelő tréningeket biztosít a szervezet munkatársainak a NAIH határozatain alapuló esettanulmányok felhasználásával.
Részt vesz az adatvédelmi incidensek kivizsgálásában és a felügyeleti hatóság fele történő jelentések elkészítésében és azzal kapcsolatos konzultációkban.
A külső adatvédelmi tisztviselő az érintetti megkeresésekről köteles a Megbízó első számú vezetőjét és a belső adatvédelmi felelőst tájékoztatni. Az adatvédelmi felelőst feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség és az adatok bizalmas kezelésére vonatkozó kötelezettség köti.
Külső adatvédelmi tisztviselő elérhetősége:

Név: **Tóth Szilárd ItJump Kft.**
Postai elérhetőség: 1082 Budapest, Corvin köz 4. 4. em. 6.
Elektronikus elérhetőség: szilard.toth@itjump.hu
Telefon szám: +36 30 411 5217

6.2. A belső Adatvédelmi felelős feladatai

A belső adatvédelmi felelős a szervezet napi munkája során gyűjti és továbbítja az adatvédelemmel, információbiztonsággal kapcsolatos észrevételeit és esetleges rendkívüli eseményekkel kapcsolatos információit a külső adatvédelmi tisztviselőnek. Részt vesz az esetlegesen szükséges, az adatvédelmi hatásvizsgálatra történő felkészítésben, valamint nyomon követi a hatásvizsgálat rendelet szerinti elvégzését. A belső adatvédelmi felelős

feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi. Részt vesz a tájékoztatók rendszeres és szükségszerűvé váló felülvizsgálatában elkészítésében, amelybe a külső adatvédelmi tisztviselő bevonásával biztosítja a szakmai felügyeletét a tájékoztatóknak. Részt vesz az adatvédelmi auditok előkészítésében, lebonyolításában. Napi tevékenysége kapcsán a szervezeten belül ellenőrzi az információbiztonsági megfelelőséget és szabályozottságot, továbbá lépéseket tesz a hiányosságok megszüntetése érdekében. Ellenőrizheti az információbiztonság szabályozottságát, betartását, felülvizsgálatát. Ellenőrzi a célok, jogalapok és tárolási idők helyes meghatározását, vezeti a nyilvántartásokat. Ellenőrzi az érintettek önrendelkezési jogainak érvényesülését. Részt vesz az adatvédelmi incidensek kivizsgálásában és a felügyeleti hatóság fele történő jelentések elkészítésében és azzal kapcsolatos konzultációkban. Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi felelőshöz fordulhatnak

Belső adatvédelmi felelős elérhetősége:

Név: Kovács Erika gazdasági igazgató
Postai elérhetőség: 1094 Budapest, Páva u. 10-12.
Elektronikus elérhetőség: Kovacs.Erika@concertobudapest.hu
Telefon szám: +36 1 215 5770

7. A szervezet adatkezelési folyamatai

7.1. A Szervezet működésével kapcsolatos adatkezelési tevékenység

Az ügyvitelhez kapcsolódó adatkezelés az ügy (bejelentés) nyilvántartásához (érkeztetéséhez, iktatásához) kapcsolódó számviteli feladatok ellátásához, feldolgozásához kapcsolódik. Alapvető célja: az adott üzleti folyamathoz tartozó tevékenységek lefolytatásához, az adatkezelés szereplőinek azonosításához és a művészeti és ismeretterjesztési közfeladataihoz, kiértékeléséhez a szervezet stratégiai céljaihoz szükséges adatokat biztosítsa. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban és az ügyviteli segédletekben szerepelnek; kezelésük ebből a célból csak az alapul szolgáló irat tárolási idejének lejáratáig, azaz selejtezéséig lehetséges.

Az Érintetti tájékoztatók tekintetében kiemelésre kell, hogy kerüljön, hogy a számviteli, pénzügyi folyamatok (kiemelten a számlával vagy pénzügyi bizonylat kiállításával) tekintetében tárolt és kezelt személyes adatok esetén a jogszabályi környezet alapján meghatározott megőrzési kötelezettség terheli a Szervezetet. A jogszabályi jogalap alapján nyilvántartott személyes adatok esetében a jogszabályban meghatározott őrzési időt követően meg kell semmisíteni vagy a személyes adatok tekintetében anonimizálni kell. A nyilvántartási célú adatkezelés az Uniós és tagállami szabályozási környezetben, továbbá más jogszabályokban előre meghatározott adatkörök alapján gyűjtött adatfajtákból álló adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét.

7.2. A Szervezettel munkavégzésre irányuló jogviszonyban állók foglalkoztatásához kapcsolódó kötelező nyilvántartási adatkezelése

Célja A foglalkoztatáshoz kapcsolódó és a munkáltatót terhelő jogszabályi kötelezettségeinek teljesítése.
Jogalap: A rendelet 6. cikk (1) c) pontja/jogszabályi jogalap
Érintettek kategóriái Alkalmazottak
Kezelt személyes adatok kategóriái

- Személyazonossághoz kapcsolódó adatok,
- elérhetőségi adatok,
- azonosító adatok,
- gazdasági, pénzügyi adatok,
- hivatalos okmányok

Tervezett adattárolási határidő Jogszabályban előírt időtartam
3. Országba továbbítás címzettje Nincs továbbítás
Jogok érvényesíthetősége Érintett írásbeli kérelmére az adatkezelő végzi

Jogszabályi kötelezettség alapján a Mt. (Munka Törvénykönyv) és a Polgári Törvénykönyv szabályai, a foglalkoztatottakra vonatkozó adózási jogszabályokban meghatározott szabályok, valamint az egészségbiztosítási és a nyugdíjellátásra vonatkozó jogszabályoknak megfelelő módon és ideig a Munkáltató/Megbízó a Munkavállaló/Megbízott következő személyes adatait kezeli és tárolja:

- Családi és utónév
- Születési név
- Anyja neve
- Születési hely
- Születési idő
- Lakcím
- Levelezési cím
- Személyazonosító igazolvány okmányazonosító
- Személyi azonosító
- Állampolgárság
- Bankszámlaszám
- Adóazonosító jel
- Magánnyugdíjpénztári adatok (név és kezdet)
- Társadalombiztosítási azonosító jel
- Kiskorú gyermek neve
- Kiskorú gyermek születési ideje
- Kiskorú gyermek születési helye
- Kiskorú gyermek anyja neve
- Kiskorú gyermek adóazonosító jele (ha van)

7.2.1. A Munkáltató/Megbízó jogos érdekkörében kezelt és nyilvántartott adatok adatkezelései

Célja: Munkáltatói és munkavállalói jogok és érdekek érvényesítése, a szervezet hatékony működésének biztosítása
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Alkalmazottak
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- azonosító adatok
- elérhetőségi adatok

Tervezett adattárolási határidő: Munkaviszony megszűnését követő 5 év, jogszabályban előírt időtartam
3. Országba továbbítás címzettje: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.2.1.1. Munkáltató/Megbízó munkakörhöz kapcsolódó elvárásai

A munkaviszonnyal/megbízási jogviszonnyal kapcsolatban a Munkáltató/Megbízó jogos érdekkörében a Munkavállaló/Megbízott adatait a működéshez köthető szerződésekben, mint kapcsolattartó megadhatja ezekben az esetekben az alábbi adatok kerülnek megadásra:

- családi és utónév
- Munkáltató/Megbízói elérhetősége
- hivatali e-mail cím
- telefonszám
- hivatali fax

A kapcsolattartói adatokat a természetes személy jogviszonyának megszűnésekor törli és új kapcsolattartót jelöl ki. Az eredeti szerződésben rögzített személyes adatokat jogos érdek jogalapján a szerződés megszűnéséig, illetve annak jogszabályban előírt idejéig tárolja, de nem kezeli.

A munkaviszonnyal/megbízási jogviszonnyal kapcsolatban a Munkáltató/Megbízó jogos érdekkörében nyilvántarthatja, kezelheti a Munkavállaló/Megbízott jogviszonyához kapcsolódó jogszabályi előírásnak, vagy a munkáltató/megbízó jogos érdekkörében a munkakör/megbízotti jogviszony betöltési feltételeül szabott végzettséget igazoló dokumentumok másolatát, illetve azok keletkezéséhez kapcsolódó adatait.

7.2.1.2. A Munkáltató/Megbízó a jogviszony tekintetében az egyéb jogszabályban elő nem írt adatokat is kezelhet munkakörtől függően, ezek a következők:

- személyes okmányok azonosítói (személyazonosító igazolvány, lakcímet igazoló hatósági igazolvány, adóigazolvány, TAJ kártya)
- a munkakörhöz kötődő büntetlen előélet igazolásának dokumentuma
- iskolai végzettséget, nyelvtudást igazoló dokumentumok azonosítói

Ezen adatokat, iratokat a jogviszony megszűnését követően törölni, megsemmisíteni köteles a nyilvántartó.

7.2.1.3. Kiküldetés

A munkaviszonnyal kapcsolatban a Munkáltató/Megbízó jogos érdekkörében a Munkavállaló/Megbízott jogviszonyához kapcsolódó esetleges külföldi, belföldi kiküldetéséhez a Munkáltató/Megbízó kérheti és nyilvántarthatja a Munkavállaló/Megbízott úti okmány azonosítóit, a magán személygépkocsi használata esetében a gépjármű azonosítására és jogszabályban meghatározott elszámoláshoz szükséges és nyilvántartására vonatkozó adatokat, és a szervezés lebonyolítás kapcsán felmerülő egyéb szükséges adatokat (az adattakarékosság elvének fenntartása mellett). A szükséges egyéb adatok a következők lehetnek:

- útlevél szám
- személyi igazolvány szám
- személygépjármű rendszáma
- gépjármű forgalmi adatai

7.2.1.4. Képzéséhez

Nyilvántarthatja és kezelheti Munkáltató/Megbízó által előírt, kezdeményezett, vagy engedélyezett, finanszírozott képzésekhez, továbbképzésekhez, azok megszervezéséhez szükséges személyes adatokat (azokról másolatot nem készíthet, da a felsorolt adatokat nyilvántarthatja, vagy az érintettet az eredeti dokumentum bemutatására kötelezheti):

- legmagasabb iskolai végzettség
- tevékenység gyakorlásához előírt szakirányú végzettség
- egyéb végzettséget igazoló dokumentumok

Nyilvántartható adatok:

- végzettség megszerzésének helye, intézménye
- tanulmányok kezdete, vége
- dokumentum száma
- végzettséghez kapcsolódó személyes adatok

Nyelvtudás adataival kapcsolatosan keletkezett adatok:

- nyelv
- kapcsolódó vizsgaszint
- megszerzés időpontja

7.2.1.5. Munkáltató/Megbízói eszközök nyilvántartása

Személyes használatú eszköz

A tevékenységi körhöz tartozó munkaeszközök tekintetében a Munkáltató/Megbízó jogos érdek jogalapra tekintettel nyilvántartást vezet a Munkavállaló/Megbízott számára biztosított eszközök esetében. A személyes használatra átadott eszközök adatai mellett nyilvántartja a személyes adatai közül:

- családi és utónév

Adattárolás

Az adattárolásra alkalmas eszközök esetében a Munkavállaló/Megbízott saját célra a jogviszonyra jellemző annak keletkezését meghatározó dokumentumokban (megbízási, munkaszerződés stb.) engedélyezheti az eszköz magáncélra történő használatát. A korlátozás módjától mértékétől függetlenül Munkáltató/Megbízó az eszközök mentéséről, az eszközön tárolt adatok mentéséről, vagy azok törléséről az eszköz helyzetének meghatározásának jogainak fenntartása mellett bármikor mentést vagy törlést kezdeményezhet.

Adatkezelő gépjárműve

Munkáltató/Megbízó tulajdonát képező gépjármű használati joga esetén a munkavállaló/megbízott adatai közül nyilvántartásba kerülnek az alábbi személyes adatok:

- a Munkavállaló/Megbízott vezetői engedély száma
- érvényességének dátuma

Az eszköznyilvántartáshoz felhasznált adatokat a természetes személy jogviszonyának megszűnését követő 5 évig tárolja, de nem kezelheti.

7.2.1.6. Munkáltató/Megbízó saját elektronikus levelező rendszerének használatáról

A Munkáltató/Megbízó saját levelezőszerver működtetését tartja fenn, a Munkavállaló/Megbízott részére személyre szabott és csoportosan használható elektronikus levélcímet biztosít. Az elektronikus levelezésben a Munkáltató/Megbízó a levelezéseket automatikusan menti és archiválja, ezért a Munkavállaló/Megbízott az elektronikus levelezési címet magáncélra használni nem jogosult. Az elektronikus levelezési címre érkező, vagy ezen keresztül küldött levelek nem minősülhetnek magánlevél titoknak.

A Munkáltató jogosult az ilyen e-mail fiók teljes tartalmát és használatát ellenőrizni, ennek során az adatkezelés jogalapja a munkáltató jogos érdeke. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek (Mt. 8.§, 52. §) ellenőrzése. Az elektronikus levélcím kiosztásához csak a természetes személy neve kerül nyilvántartásra.

7.2.1.7. Adattárolásra alkalmas informatikai eszközök ellenőrzésével kapcsolatos adatkezelés

A Társaság által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, okostelefont, adattárolásra alkalmas informatikai eszközt a munkavállaló kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát a társaság egyedi, a munkaszerződéshez kapcsolódó vagy attól független írásbeli jognyilatkozat meglétéhez köti. Ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezést nem kezelhet, és nem tárolhat. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. Amennyiben a munkavállaló a munkavégzéshez saját eszközt vesz igénybe az azon tárolt, de a munkáltató adatvagyonát képező adatokhoz a munkáltató előre jelzett kéréssel jogosult hozzáférni, ellenőrizni. A munkáltató a saját eszközön tárolt magán jellegű adatok megismerésére nem jogosult.

7.2.1.8. A munkahelyi internethasználat ellenőrzésével kapcsolatos adatkezelés

A munkavállaló csak a munkaköri feladatával kapcsolatos honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja. A munkaköri feladatként a társaság nevében elvégzett internetes regisztrációk jogosultja a társaság, a regisztráció során a társaságra utaló azonosítót, jelszót kell alkalmazni. Amennyiben a személyes adatok megadása is szükséges a regisztrációhoz, a munkaviszony megszűnésekor azok törlését köteles kezdeményezni a társaság. A munkavállaló munkahelyi internet használatát a munkáltató ellenőrizheti.

7.2.1.9. Cégkapu/ hivatali kapu használat

A Munkáltató/Megbízó elektronikus kommunikációra kötelezett szervezet, ezért a Munkáltató/Megbízó rendelkezik:

Cégkapuval/Hivatali kapuval, a Munkavállaló/Megbízott feladatkörétől függően kötelezettségként vagy lehetőségként elektronikus kommunikációt kezdeményezhet a Munkáltató/Megbízó több felhasználós e-kapuján keresztül. Az e-kapu használatához a vezetői utasítás alapján kell a Munkavállaló/Megbízott az e-kapu felelősnek hozzárendelni ügykezelőként. A hozzáférés létrehozása érdekében a Munkavállalónak/Megbízottnak a következő adatokat kell megadni:

- családi és utónév
- születési név

- anyja neve
- születési hely
- születési időpont

Az e-kapu használati jogának, vagy a Munkáltatóval/Megbízóval fenntartott jogviszony megszüntetésének az adatok törlése közvetlen következménye.

7.2.1.10. Elektronikus aláírások

Az elektronikus aláírások személyes adatokat tartalmaznak. A Munkavállaló/Megbízott feladatköri feladatainak ellátása közben kötelezetté válhat elektronikus aláírásra. Az elektronikus aláírás használata elkerülhetetlenné válhat a betöltött pozícióhoz, a Munkáltató/Megbízó jogos érdekében, vagy törvényi előírásoknak eleget téve. A Munkáltató/Megbízó a munkakör betöltését Ügyfélkapu meglétéhez kötheti és ebből kifolyólag a Munkavállaló/Megbízott az elektronikus kommunikáció során köteles lehet az ügyfélkapu használatához kötött AVDH aláírását munkakörében használni. A Munkavállaló/Megbízott feladatkörének betöltése során elektronikus aláírásra lehet kötelezett olyan dokumentumok esetében is, ahol az AVDH aláírás nem alkalmazható. Ilyen esetekben a Munkáltató/Megbízó üzleti aláírókártyával láthatja el a Munkavállalót/Megbízottat. A Munkáltató/Megbízó által biztosított üzleti aláírókártya a tanúsítványban rögzített pozíciónak megfelelő aláírási kötelezettségek esetében használható.

7.2.2. Adatkezelő alkalmazottainak marketing és ismeretterjesztés célú hang- és képfelvételeinek kezelése

Célja: A foglalkoztatott művészek hang- és képfelvételeiben rejlő marketing értékek, ismeretterjesztési lehetőségeinek kihasználása
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Alkalmazottak
Kezelt személyes adatok kategóriái:

- képfelvétel
- hangfelvétel

Tervezett adattárolási határidő: Az adatkezelő Szervezetének történeti, történelmi jelentőségűnek nem tekinthető adatok esetében maximum 5 év
Harmadik országba továbbítás címzettje: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.2.3. Kép- és hangfelvétel készítése saját szervezésű zenei és kulturális eseményeken

Cél: Weboldalon, közösségi médiumokban, marketing eszközökön való megjelenítés a szervezet zenei kulturális tevékenységének népszerűsítése és az adatkezelő alaptevékenységéből fakadó kulturális ismeretterjesztési céljainak teljesítése érdekében
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Alkalmazottak, ügyfelek, diákok
Kezelt személyes adatok kategóriái:

- képfelvétel
- hangfelvétel

Tervezett adattárolási határidő: Az adatkezelő szervezetének történeti, történelmi jelentőségűnek nem tekinthető adatok esetében maximum 5 év
Harmadik országba továbbítás címzettje: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.2.3.1. Művészeti és marketing jellegű kép- és hangfelvételek

Az Adatkezelő (Munkáltató/Megbízó) tevékenységi profiljába tartozó művészeti és ismeretterjesztő tevékenység szükségessé teszi a rendszeres kép- és hangfelvétel készítését a felkészülés, vagy éppen az adott esemény lebonyolítása során, hogy a szervezet tevékenységét népszerűsítse, és koncertjei látogatottságát növelje. A munkavállaló (kiemelten, ha művészeti vagy ahhoz közvetlenül kapcsolódó munkakört lát el) tudomásul veszi, hogy az adatkezelő jogos érdeke a felvételek elkészítése és felhasználása, mely ellen egyedi esetekben az érintett jogosult tiltakozást bejelenteni. A felvételek az adatkezelő által preferált közösségi oldalakon, saját weboldalán, a papíralapú és elektronikus célú marketing anyagokban kerülnek felhasználásra. A történelmi, kutatási, levéltári érdeklődésre számot tartó felvételek megőrzése tekintetében a tárolási idő konkrétan a cél megszűnéséig vagy az érintett tiltakozásának elbírálásáig kerül megőrzésre anélkül, hogy a tárolhatóság vagy az adattakarékosság elvét sértené.

7.2.3.2. Elektronikus hírközlő eszközökön folytatott üzleti kapcsolattartások kép- és hang felvételeinek kezelése

A Munkáltató/Megbízó üzleti érdekeinek és kapcsolattartásainak folyamán elektronikus távközlési eszköz igénybevételével lebonyolított szervezeten belüli képzések megbeszélések, illetve üzleti partnerekkel folytatott tárgyalások esetében az eseményről felvételt készít és minden eseménytípushoz megfelelő adatkezelési tájékoztatót készít. A felvételek tárolási idejét az esemény céljának, típusának megfelelően határozza meg. A résztvevő Munkavállaló/Megbízott joggal számíthat rá, hogy ezen eseményeken az ő kép- és hangfelvételei is rögzítésre, majd a tárolási idő lejártát követően törlésre kerülnek.

7.2.4. Adatkezelő alkalmazottainak adatkezelési nyilvántartása (különleges egészségügyi adatai)

Cél: A megváltozott munkaképességű munkavállalók rehabilitációs hozzájárulás kiváltását érintő adatszolgáltatáshoz kapcsolódó kötelezettség teljesítése
Jogalap: A rendelet 6. cikk (1) a) pontja Hozzájárulás
Érintettek kategóriái: Alkalmazottak
Kezelt személyes adatok kategóriái: Különleges adatok/ Egészségügyi adatok
Címzettek kategóriái: hatóságok, felügyeleti szervek
Tervezett adattárolási határidő: Hozzájárulás visszavonásáig, illetve a munkaviszony megszűnésének évét követő 5 évig (adóhatósági ellenőrzési kötelezettség megszűnéséig)
Harmadik országba továbbítás címzettje: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.2.5. Munkavállalók személyes adatainak átadása adatfeldolgozóknak

A Munkavállaló/Megbízott tudomásul veszi, hogy a Munkaadó/Megbízó tevékenységi körében alvállalkozókkal adatfeldolgozókkal áll kapcsolatban. A Munkáltató/Megbízó a Munkavállaló/Megbízott személyes adatait adatfeldolgozás céljából továbbítja (az

adattakarékosság elvének figyelembevételével) a következő adatfeldolgozók számára és céllal:

Üzemorvos: szakmai egészségügyi alkalmasság ellenőrzése, fenntartása
Számviteli szolgáltató: számviteli, könyvviteli feladatok ellátása
Bérszámfejtő: a bérek számfejésével és utalás előkészítése
Könyvvizsgáló: az Adatkezelő célszerű és észszerű gazdálkodásának vizsgálata
Belső ellenőr: a szervezet folyamatait és nyilvántartásait törvényességi szempontok alapján történő vizsgálata
Informatikai rendszerszolgáltató: informatikai fejlesztés és üzemeltetés
Informatikai eszköz-üzemeltető: rendszerüzemeltető

7.2.6. Adatok átadása címzettek részére

Nemzeti Adó és Vámhivatal
Megyei Kormányhivatal Nyugdíjbiztosítási Igazgatósága
Megyei Kormányhivatal Egészségbiztosítás szerve
Egyéb, jogszabály alapuló adatközlési kötelezettség címzettje

7.3. A munkaviszonyban nem álló érintettekre vonatkozó adatkezelési folyamatai

7.3.1. Kép- és hangfelvétel készítése saját szervezésű zenei és kulturális eseményeken

Cél: Weboldalon, közösségi médiumokban, marketing eszközökön való megjelenítés a szervezet zenei kulturális tevékenységének népszerűsítése és az adatkezelő alaptevékenységéből fakadó kulturális ismeretterjesztési céljainak teljesítése érdekében
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Alkalmazottak, ügyfelek, diákok
Kezelt személyes adatok kategóriái

- képfelvétel
- hangfelvétel

Tervezett adattárolási határidő: Az adatkezelő szervezetének történeti, történelmi, jelentőségűnek nem tekinthet adatok esetében maximum 5 év
Harmadik országba továbbítás címzettje: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.2. Pénzügyi, számviteli kötelezettségek teljesítésével kapcsolatos adatkezelés

Adatkezelés célja: Koncertek szervezéséhez, online és offline jegy- és bérletértékesítéshez kapcsolódó számlázási adatok felhasználásával az adatkezelő pénzügyi számviteli és adózási kötelezettségeinek teljesítéséhez, azok ellenőrzéséhez kapcsolódó feladatok teljesítése.
Jogalap: A rendelet 6. cikk (1) c) pontja/ jogszabályi jogalap
Érintettek kategóriái: Ügyfelek, diákok
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok

- elérhetőségi adatok
- azonosító adatok
- gazdasági, pénzügyi adatok

Címzettek kategóriái: hatóságok, felügyeleti szervek
Tervezett adattárolási határidő: számviteli bizonylat keletkezését követő 8. év végéig
Harmadik országba továbbítás: Nincs továbbítás
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.3. Offline és Online jegy-, bérletértékesítés saját vagy partner weboldalon

Adatkezelés célja: Az előadások módosulásával és elmaradásával kapcsolatos információk eljuttatása a jegyvásárlóhoz.
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Ügyfelek, diákok
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- elérhetőségi adatok

Harmadik országba továbbítás: Nincs továbbítás
Tervezett adattárolási határidő: Jegyvásárlást követő 5 év
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.4. Zenei kulturális események szervezésével kapcsolatos adatkezelés

Adatkezelés célja: A sikeres koncertek szervezésének támogatása látogatottságának növelése.
Jogalap: A rendelet 6. cikk (1) f) pontja/ Az adatkezelő vagy egy harmadik fél jogos érdeke
Érintettek kategóriái: Ügyfelek, diákok
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- elérhetőségi adatok

3. Országba továbbítás: nincs továbbítás
Tervezett adattárolási határidő: jegyvásárlást követő 5 év
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.5. A szerződéses partnerekkel kapcsolatos adatok kezelése

Adatkezelés célja: A szerződés teljesítéséhez szükséges kommunikációs csatornák hatékony működtetése érdekében szükséges adatkezelés.
Jogalap: A rendelet 6. cikk (1) b) pontja/ Szerződéses jogalap
Érintettek kategóriái: Ügyfelek
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- elérhetőségi adatok

Harmadik országba továbbítás: Nincs továbbítás
Tervezett adattárolási határidő: Jegyvásárlást követő 5 év
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.6. A szerződéses partnerekkel kapcsolatos számviteli, pénzügyi adatok kezelése

Adatkezelés célja: Az Adatkezelő pénzügyi, számviteli és adózási kötelezettségeinek teljesítéséhez, azok ellenőrzéséhez kapcsolódó feladatok teljesítése
Jogalap: A rendelet 6. cikk (1) c) pontja/ jogszabályi jogalap
Érintettek kategóriái: Ügyfelek
Kezelt személyes adatok kategóriái:

- Személyazonossághoz kapcsolódó adatok
- Elérhetőségi adatok
- Azonosító adatok
- Gazdasági, pénzügyi adatok

Címzetteknek továbbítás: hatóságok és felügyeleti szervek felé
Harmadik országba továbbítás: Nincs továbbítás
Tervezett adattárolási határidő: Számviteli bizonylat keletkezését követő 8. év végéig
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

7.3.7. Hírlevél szolgáltatáshoz kapcsolódó adatkezelés

Adatkezelés célja: A feliratkozókkal történő közvetlen tájékoztatási és ismeretterjesztési célú kapcsolattartás hatékony támogatása. A zenekedvelő közönség és a zene iránt érdeklődők érdeklődésének megfelelő struktúrában szeretné az adatkezelő azokat a tevékenységi körébe tartozó információkat, akciókat és marketing elemeket, tájékoztatásokat, lehetőségeket eljuttatni, amelyek az adatkezelő és az értékesítő marketing szervezet hatékonyságát támogatják.
Jogalap: A rendelet 6. cikk (1) a) pontja/ Hozzájárulás jogalap
Érintettek kategóriái: Feliratkozók
Kezelt személyes adatok kategóriái:

- Személyazonossághoz kapcsolódó adatok
- Elérhetőségi adatok

Tervezett adattárolási határidő: Hozzájárulás visszavonásáig
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi
Harmadik országba továbbítás: nincs továbbítás

7.3.8. Vendégművészek utaztatásával elszállásolásával kapcsolatos adatkezelési folyamatok

Adatkezelés célja: A meghívott hazai és külföldi vendégművészek számára olyan ügyintézési szolgáltatások nyújtása, amely vonzóbbá teszi az adatkezelőnél biztosított fellépési lehetőséget
Jogalap: A rendelet 6. cikk (1) a) pontja/ Hozzájárulás jogalap
Érintettek kategóriái: Ügyfelek
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- elérhetőségi adatok
- azonosító adatok

Címzetteknek továbbítás: szállás szolgáltatók
Tervezett adattárolási határidő: Hozzájárulás visszavonásáig
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi

Harmadik országba továbbítás: Nincs továbbítás

7.3.9. Zenei gyermektábor lebonyolításához kapcsolódó adatkezelési folyamat

Adatkezelés célja: A táboroztatás eseményeinek és népszerűsítésének kép- és hanganyagon történő megőrzése, a népszerűsítés és táborozókkal kapcsolatos szülői és gondviselői tájékoztatás és közvetlen kapcsolattartás.
Jogalap: A rendelet 6. cikk (1) a) pontja/ Hozzájárulás jogalap
Érintettek kategóriái: Kiskorúak és gondviselőik
Kezelt személyes adatok kategóriái:

- személyazonossághoz kapcsolódó adatok
- elérhetőségi adatok
- azonosító adatok
- kép, és hanganyagok

Tervezett adattárolási határidő: Hozzájárulás visszavonásáig
Jogok érvényesíthetősége: Érintett írásbeli kérelmére az adatkezelő végzi
Harmadik országba továbbítás: Nincs továbbítás

7.4. Egyéb weboldali és közösségi média felületeken alkalmazott adatkezelés folyamatok

7.4.1. GOOGLE ADS KONVERZIÓKÖVETÉS HASZNÁLATA

Concerto a „Google Ads" nevű online reklámprogramot használja, továbbá annak keretein belül igénybe veszi a Google konverziókövető szolgáltatását. A Google konverziókövetés a Google Inc. elemző szolgáltatása (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; „Google").
Amikor Felhasználó egy weboldalt Google-hirdetés által ér el, akkor egy a konverziókövetéshez szükséges cookie kerül a számítógépére. Ezeknek a cookie-knak az érvényessége korlátozott, és nem tartalmaznak semmilyen személyes adatot, így a Felhasználó nem is azonosítható általuk.
Amikor a Felhasználó a weboldal bizonyos oldalait böngészi, és a cookie még nem járt le, akkor a Google és az adatkezelő is láthatja, hogy Felhasználó a hirdetésre kattintott.
Minden Google Ads ügyfél másik cookie-t kap, így azokat az Ads ügyfeleinek weboldalain keresztül nem lehet nyomon követni.
Az információk – melyeket a konverziókövető cookie-k segítségével szereztek – azt a célt szolgálják, hogy az Ads konverziókövetést választó ügyfeleinek számára konverziós statisztikákat készítsenek. Az ügyfelek így tájékozódnak a hirdetésükre kattintó és konverziókövető címkével ellátott oldalra továbbított felhasználók számáról. Azonban olyan információkhoz nem jutnak hozzá, melyekkel bármelyik felhasználót azonosítani lehetne.
Ha nem szeretne részt venni a konverziókövetésben, akkor ezt elutasíthatja azáltal, hogy böngészőjében letiltja a cookie-k telepítésének lehetőségét. Ezután Ön nem fog szerepelni a konverziókövetési statisztikákban.
További információ, valamint a Google adatvédelmi nyilatkozata az alábbi oldalon érhető el: www.google.de/policies/privacy/

7.4.2. A GOOGLE ANALYTICS ALKALMAZÁSA

A www.concertobudapest.hu honlap a Google Analytics alkalmazást használja, amely a Google Inc. („Google") webelemző szolgáltatása. A Google Analytics úgynevezett „cookie-kat", szövegfájlokat használ, amelyeket a számítógépére mentenek, így elősegítik a Felhasználó által látogatott weblap használatának elemzését.

A Felhasználó által használt weboldallal kapcsolatos cookie-kkal létrehozott információk rendszerint a Google egyik USA-beli szerverére kerülnek és tárolódnak. Az IP-anonimizálás weboldali aktiválásával a Google a Felhasználó IP-címét az Európai Unió tagállamain belül vagy az Európai Gazdasági Térségről szóló megállapodásban részes más államokban előzőleg megrövidíti.

A teljes IP-címnek a Google USA-ban lévő szerverére történő továbbítására és ottani lerövidítésére csak kivételes esetekben kerül sor. Eme weboldal üzemeltetőjének megbízásából a Google ezeket az információkat arra fogja használni, hogy kiértékelje, hogyan használta a Felhasználó a honlapot, továbbá, hogy a weboldal üzemeltetőjének a honlap aktivitásával összefüggő jelentéseket készítsen, valamint, hogy a weboldal- és az internethasználattal kapcsolatos további szolgáltatásokat teljesítsen.

A Google Analytics keretein belül a Felhasználó böngészője által továbbított IP-címet nem vezeti össze a Google más adataival. A cookie-k tárolását a Felhasználó a böngészőjének megfelelő beállításával megakadályozhatja, azonban felhívjuk figyelmét, hogy ebben az esetben előfordulhat, hogy ennek a honlapnak nem minden funkciója lesz teljeskörűen használható. Megakadályozhatja továbbá, hogy a Google gyűjtse és feldolgozza a cookie-k általi, a Felhasználó weboldalhasználattal kapcsolatos adatait (beleértve az IP-címet is), ha letölti és telepíti a következő linken elérhető böngésző plugint: https://tools.google.com/dlpage/gaoptout?hl=hu

8. Adatkezelési folyamatba épített adatvédelem

8.1. Az adatkezelői tevékenységbe épített védelem

A feladatok elvégzéséhez olyan szervezetet működtet, amely feladatspecifikusan a legkisebb erőforrásból a hatékony és számonkérhető feladat- és felelősség megosztásra épül.

Az adatkezelés során a rögzítéstől a riportolásig minden munkafolyamat kiosztását a munkakörökhöz illesztett jogosultsági rendszerrel támogatja, folyamatosan vizsgálja, felülvizsgálja a strukturált adatkezeléssel megbízott kollégák jogosultságait és a belső (szervezeten belüli adatáramlás) hatékonyságát és kockázatát.

Az Adatkezelők a jogviszonyukhoz kapcsolódó tájékoztatás mellett, rendszeres és tudatos adatkezelési szemlélet kialakítását célzó képzésen és továbbképzésen vesznek részt.

Az adatkezelés során az Adatkezelők kötelesek az adattakarékosság elvét betartani és követni. Adatkezelői tevékenységük során minimalizálni kötelesek a munkahelyi nevesített informatikai eszközeik helyi tárolókapacitásán elhelyezett személyes adatok mennyiségét. Saját adathordozóra tilos a Szervezet adatvagyonát képező, vagy személyi adatokat érintő adathalmazt vagy dokumentumot menteni, tárolni.

9. Adatfeldolgozók

A Szervezet kapcsolati hálójából Adatfeldolgozónak számít az személy vagy szervezet, aki/amely az Adatkezelővel kötött szerződése alapján – beleértve a jogszabályi környezet rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. A Szervezet által tárolt adatok köréhez részben, vagy egészben hozzáfér, a hozzáférése kizárólag a szerződés idejére szól, a Szervezet részére az adatokon bármilyen módosítást feldolgozást csak és kizárólag írásos utasításra végez. Feladata, hogy az Adatkezelőnél hatékonyan nem működtethető vagy nem meghonosítható szaktudást és speciális feladatok ellátását, szolgáltatásokat biztosítsa.

9.1. Informatikai rendszerek és szoftverszolgáltatás területét érintő adatfeldolgozók

Számlázz.hu:
Üzemeltető: KBOSS.hu Kft. (adószám: 13421739-2-13, cégjegyzékszám: 13-09-101824, székhely: 2000 Szentendre, Táltos u. 22/b)

Kulcs-Soft
Üzemeltető: Kulcs-Soft Számítástechnikai Nyrt. (székhely: 1022 Budapest, Törökvész út 30/A., adószám: 13812203-2-41, közösségi adószám: HU13812203, cégjegyzékszám: 01-10-045531).

jegy.hu
Üzemeltető: INTERTICKET Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (székhely: 1139 Budapest, Váci út 99. 6. em., adószám: 10384709-2-41, cégjegyzékszám: 01-09-736766).

Rendszergazdai feladatok
Üzemeltető: Poli Computer PC Kft. (székhely: 2071 Páty, Fazekas M. u. 17., adószám: 11820534-2-13, cégjegyzékszám: 13-09-081942).

Weboldal, tárhelyszolgáltatás biztosítás és üzemeltetés
E-Solution Kft. (székhely: 1119 Budapest, Fehérvári út 131. Fsz. 3., adószám: 12596535-2-43, cégjegyzékszám: 01-09-694209) mint adatfeldolgozó végzi.

9.2. A számviteli feladatok

Könyvelés
Számviteli adatfeldolgozó: Csöngedi és Társa Kft. (székhely: 1035 Budapest, Szél u 17. 9. em. 50., adószám: 12000090-2-41, cégjegyzékszám: 01-09-366534).

Bérszámfejtés
STARJOBS Magyarország Humánszolgáltató Kft. (székhely: 2724 Újlengyel, Kossuth Utca 138., adószám: 12642870-2-13, cégjegyzékszám: 13-09-100398).

9.3. Marketing és reklám tevékenység fontosabb adatfeldolgozói

Grafikus
Efergefer Kft. (székhely: 2030 Érd, Selmeci utca 55. fszt. 1., adószám: 22764225-2-13, cégjegyzékszám: 13-09-189043).

Nyomda
PAUKER HOLDING Kft. (székhely: 1047 Budapest, Baross u. 11-15., adószám: 12739882-2-41, cégjegyzékszám: 01-09-701128).

9.4. Interticket Kft. és a Concerto Akadémia Nonprofit Kft. együttműködése

A felek önálló és egymástól független informatikai rendszerekkel és adatkezelési folyamatokkal rendelkeznek. (a Concerto bérli az Interticket által fejlesztett rendszer bizonyos moduljait és az abba rögzített **tranzakcióhoz és beléptetéshez kapcsolódó** adatok adatkezelője önálló adatkezelőként az Interticket is és a Concerto is).

- **számlakibocsátáshoz kapcsolódó adatkezelés:** mint bizományos a számlázást az Interticket adatkezelő ként végzi, a saját jegypénztárból, de az Interticket rendszerén kiállított számlák tekintetében az adatkezelő a Concerto.

- **a jegyvásárlási tranzakcióhoz és beléptetéshez kapcsolódó adatkezelés:** ebben az adatkezelési folyamatban mindkét fél önálló adatkezelő -mindkét fél megismerheti és hozzáférhet az adatokhoz, amelynek tárolása az Interticket infrastruktúráján van tárolva.
  Ezekből az adatokból történik a koncertekkel kapcsolatos tájékoztatás.

- **egyéb adatkezelések:**
  - hírlevél rendszer
  - lojalitási programok kezelése
  - ajándékkártya
  - kényelmi szolgáltatás

9.5. Adatfeldolgozók ellenőrzési folyamatai

Az Adatfeldolgozók ellenőrzését évente egy alkalommal, szúrópróbaszerűen, az Adatkezelő kijelölt munkatársa vagy alvállalkozója végzi el. Az audit kizárólag a vállalkozási, szolgáltatási szerződésben szereplő folyamatokra terjed ki. Az audit megtartás előtt az adatkezelő 2 héttel korábban köteles jelezni az adatfeldolgozó felé az audit időpontját. Az audit tartalmát az alapszerződéssel összhangban kell összeállítani és elvégezni az audit jegyzőkönyveit az adatkezelő irattárában elhelyezni.

10. Harmadik országgal kapcsolatos rendelkezések

A Szervezet harmadik országbeli adatkezelőknek, Adatfeldolgozóknak, egyéb Címzetteknek vagy nemzetközi szervezeteknek nem továbbít adatot.

Adatfeldolgozói kapcsolatrendszerében, és azok alvállalkozói esetében sem merül fel harmadik országbeli adatkezelő vagy adatfeldolgozó folyamat. A Szervezet felhívja az Adatfeldolgozók figyelmét, hogy az esetleges harmadik országbeli adatfeldolgozási tevékenység megkezdése előtt, bejelentéssel kötelesek élni a Szervezet felé és bizonyítania kell, hogy nem sérülhet a természetes személyeknek az Unióban e rendelettel biztosított védelem szintje. A harmadik országokba és a nemzetközi szervezetekhez való továbbítás csak az Uniós GDPR Rendelet teljes betartása mellett hajtható végre. A továbbításra akkor kerülhet csak sor, ha az Adatkezelő vagy az adatfeldolgozó – e szabályzat egyéb rendelkezéseire is figyelemmel – teljesíti az harmadik országok vagy nemzetközi szervezeteknek történő adattovábbításra vonatkozó, a Rendeletben meghatározott feltételeket.

Harmadik országgal kapcsolatos adatkezelés esetében figyelembe veszi a Rendelet vonatkozó kitételeit.

11. Adatvédelmi incidens kezelésének eljárása

Az Incidenskezelésének szabályozását a szervezetben külön elkészített rövid szabályzat szabályozza annak érdekében, hogy az incidens kezelésére vonatkozó szabályokat az adatkezelő minden munkatársa ismerje és a belső észlelés esetén késedelem nélkül megkezdődhessen az incidens következményeinek elhárítása, illetve a jogszabályi határidőn belüli bejelentés megkezdhető legyen.

11.1. Incidens észlelésének módjai

11.1.1. Adatkezelő által észlelt incidens

Azok az incidensek tartoznak ebbe a körbe, amelyek esetében az incidens bekövetkeztének tényét az adatkezelő munkavállalója érzékeli, veszi észre és a tudomásra jutást követő bejelentésig vagy az incidens elhárításáig az érintett vagy harmadik személy sem az adatkezelőnek sem a felügyeleti hatóságnak nem jelentette be.

Pl.: téves címzés (elektronikus vagy papíralapú), hackertámadás, vírusfertőzés, rendelkezésre állás sérülése, jogosulatlanul elérhető adat, adatkezelő adattárolásra alkalmas informatikai eszközének elvesztésem ellopása, az adatkezelő munkatársának saját, de munkavégzésre is használt, személyes adatokat tartalmazó adattárolásra alkalmas informatikai eszközének elvesztésem ellopása, személyes adatok tárolására használt adattárolók megsemmisülése használhatatlanná válása

11.1.2. Adatfeldolgozó által észlelt incidens

Az incidens megvalósulásáról az Adatfeldolgozó vagy annak munkatársai, illetve annak Al-adatfeldolgozói az Al-adatfeldolgozón keresztül tájékoztatják az Adatkezelőt.

Pl.: Az Adatfeldolgozó informatikai rendszerét ért hackertámadás, vírus fertőzés, rendelkezésre állás sérülése, jogosulatlanul elérhető adat, Adatfeldolgozó adattárolásra alkalmas informatikai eszközének elvesztésem ellopása, az adatfeldolgozó munkatársának saját, de munkavégzésre is használt, személyes adatokat tartalmazó adattárolásra alkalmas informatikai eszközének elvesztésem

ellopása, személyes adatok tárolására használt adattárolók megsemmisülése használhatatlanná válása.

11.1.3. Érintett vagy harmadik személy által észlelt incidens

A bekövetkezett és személyes adatok kezelését, tárolását érintő sérülésről megsemmisülésről, rendelkezésre állás megszűnéséről az Érintett vagy harmadik személy közvetlen (Adatkezelőnek vagy Adatfeldolgozónak) tett bejelentése, vagy a NAIH által a bejelentést követően érkezett tájékoztatás kérése.

11.2. Incidens besorolás kategóriái

11.2.1. Alacsony kockázattal járó incidens

A személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén.

11.2.2. Közepes kockázattal járó incidens

A személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén.

11.2.3. Magas kockázattal járó incidens

- A személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén, illetve
- az adatok körétől függetlenül minden olyan eset, amikor az incidensnek az érintettre hátrányos hatása valószínűsíthető, vagy a hátrányos következmény bekövetkezés mértéke biztos.

11.3. Az adatvédelmi incidensek típusai

11.3.1. Bizalmasság sérülésével kapcsolatos incidens

A személyes adatokat érintő incidens kockázatot jelent olyan személyes, nem nyilvános adatokra nézve, melyek közlése, megismerése lehetővé teszi az érintett azonosítását, érdekeinek, bizalmas adatainak vagy életkörülményeinek sérelmét. A személyes adatok véletlen vagy felhatalmazás nélküli közlése, vagy az ezekhez való hozzáférés az érintettre nézve kockázatot jelent.

11.3.2. Sértetlenség (integritás) sérülésével kapcsolatos incidens

A személyes adatokat érintő incidens olyan típusai, melyek a személyes adatok véletlen vagy jogtalan megváltoztatására lehetőséget biztosítanak.

11.3.3. Rendelkezésre állás sérülésével kapcsolatos incidens

A személyes adatokat érintő incidens, olyan típusai melyek a személyes adatok véletlen vagy jogtalan megsemmisítésével járnak vagy elvesztésüket, elérhetetlenségüket eredményezi. Ez egyre nagyobb kockázatot jelent, minél több olyan, csak

elektronikusan elérhető adat van. Komoly kockázatot jelent, ha papíralapon már nem áll rendelkezésre, és az adatok elvesztése - a megfelelő mentések hiányában – túl sok időt igényel a helyreállításra, vagy lehetetlenné válik.

11.4. Incidens észlelésének fogalma

Az incidens észleléséhez olyan szigorú és fontos határidő kötődik, amely szükségessé teszi a fogalom definiálását. Az észlelés időpontjának az az időpont tekinthető amikor az adatkezelő vagy annak adatfeldolgozója az incidens megtörténtéről tudomást szerez.

11.5. Adatvédelmi incidens során alkalmazandó eljárásrend

A Szervezet azon munkatársának, aki az incidensről tudomást szerez, a tudomásszerzést követően azonnal tájékoztatni köteles a belső adatvédelmi felelőst.

A belső adatvédelmi felelős felméri a helyzetet és írásban rögzíti a megismert tényeket.

- az incidens észlelésének módja (ki)
- az incidens észlelésének körülményei (mikor, mi történt, milyen személyes adatokat érint, eddig milyen lépések történtek az incidens megszüntetésére, ismétlődésének kizárására.
- az incidens mibenlétének részletes adatai
- elvégzi a tények ismeretében az elsődleges besorolását a rendkívüli eseménynek
    - kategóriája
    - típusa
    - kockázati szintje
    - majd a szabályzatban meghatározott Adatvédelmi incidens során alkalmazandó eljárásrendben meghatározott protokollt követi.

11.6. Adatvédelmi incidens során alkalmazandó eljárásrend

A belső adatvédelmi felelős felveszi a kapcsolatot az adatvédelmi incidenst észlelő személlyel, szükség esetén a bejelentővel. Eldönti, hogy az incidenshez kapcsolódó elhárítási, bejelentési folyamatba kiknek a bevonása szükséges.

Amennyiben az incidens informatikai rendszert is érint, azonnal felveszi az illetékes rendszergazdával a kapcsolatot és bevonja az elhárításba.

A belső adatvédelmi felelősnek a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

- Alacsony szintű adatvédelmi incidens: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset esetén.
- Közepes szintű adatvédelmi incidens: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset estén.
- Magas szintű adatvédelmi incidens:

- a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, más jogellenes adatkezelési incidens estén, illetve
- az adatok körétől függetlenül minden olyan eset, amikor az incidensnek az Érintettre hátrányos hatása valószínűsíthető, vagy a hátrányos következmény bekövetkezésének mértéke biztos.

11.6.1. Alacsony szintű adatvédelmi incidens eljárási folyamata

Alacsony szintű adatvédelmi incidens esetén a belső adatvédelmi felelős önállóan intézkedik az incidens megszüntetéséről és adminisztrálásáról:

- a vonatkozó rendszer rendszergazdájával (amennyiben az incidens informatikai rendszert is érint) meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

11.6.2. Közepes szintű adatvédelmi incidens eljárási folyamata

Közepes szintű adatvédelmi incidens esetén a belső adatvédelmi felelős azonnali hatállyal összehívja az incidens kezelési munkacsoportot:

- a belső adatvédelmi felelős haladéktalanul, de legkésőbb 12 órán belül munkacsoportot hív össze,
- a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- a külső adatvédelmi tisztviselő dönt a bejelentésről, szükség esetén felvesz a kapcsolatot az adatvédelmi hatósággal és elvégzi a bejelentést,
- az külső adatvédelmi tisztviselő rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában.

11.6.3. Magas szintű adatvédelmi incidens eljárási folyamata

Magas szintű adatvédelmi incidens esetén:

- a belső adatvédelmi felelős haladéktalanul, de legkésőbb 12 órán belül válságstábot hív össze
- a válságstáb meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
- a külső adatvédelmi tisztviselő dönt a bejelentésről, szükség esetén felveszi a kapcsolatot az adatvédelmi hatósággal és elvégzi a bejelentést,
- az külső adatvédelmi tisztviselő rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,
- a válságstáb meghatározza, kihirdeti az adatvédelmi incidenst követő kötelező intézkedéseket, a szabályozásban, eljárásrendekben hatályba léptetendő intézkedéseket elrendeli és visszaellenőrzi a tájékoztatási kötelezettség végrehajtását,
- az érintett területeken oktatást rendel el.

11.7. Az incidens kezelés (GDPR-ben meghatározott) általános protokollja

Az Adatkezelő tudomására jut az adatvédelmi incidens, azt **indokolatlan késedelem nélkül – és ha lehetséges legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott – bejelenteni köteles az illetékes felügyeleti hatóságnál**, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

11.8. Az adatvédelmi incidens súlyossága értékelésének fő kritériumai

- Az **Adatkezelési Környezet (AK)** vizsgálata: a megsérült adatok fajtáját veszi górcső alá, beleértve az adatkezelés valamennyi körülményét
- Az **Azonosíthatóság Mértékének (AM)** meghatározása: azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni
- A **Sérülés Körülményeinek (SK)** leírása: a sérülés körülményeit vizsgálja, elsősorban a megsérült adat biztonságának csökkenését, illetve a rosszindulatú támadásra és a szándékosságra utaló valamennyi jelet

Az ajánlás segítséget nyújt az incidensben **érintett adatok típusának meghatározásában** (egyszerű adat, pénzügyi adat, viselkedésre vonatkozó adat, érzékeny adat), az **eset körülményeinek feltérképezésében** (a veszélyességet csökkentő, illetve növelő faktorok), és végül a **veszély súlyosságának (VS) objektív mérők szerinti** megállapításában:

VS = AK x AM + SK

11.9. Az adatvédelmi incidens-nyilvántartás tartalma

Az adatkezelő a rendelet 33. cikk (5) bekezdésnek megfelelően tartja nyilván az incidenseket. A nyilvántartás minden mezője a felügyeleti hatóság (NAIH) online bejelentőjének megfelelő struktúrában kerül nyilvántartásra. Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

Nyilvántartás nyilvántartott adatai:

Sorszám	1	2	3
Adatvédelmi incidens jelentése			
A bejelentő adatai			
A bejelentő kapcsolattartása			
Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban			
Incidenshez kapcsolódó időpontok			
Az adatvédelmi incidens jellemzői			
Az adatvédelmi incidenssel érintett személyes adatok			
Az érintettek kategóriái			
Az incidens ELŐTT alkalmazott intézkedések			
Valószínűsíthető következmények			
Megtett intézkedések			

11.9.1. A nyilvántartás részletes adattartalma

0. Adatvédelmi incidens jelentése

- Bejelentés típusa
- A korábban bejelentett incidens azonosítója
- A korábbi bejelentés időpontja

1. A bejelentő adatai

1.1 Kapcsolati

- A bejelentő adatkezelő cégjegyzékszáma
- A bejelentő adatkezelő adószáma (magánszemély bejelentése esetén nem kell)
- Szervezet száma
- A bejelentő adatkezelő elnevezése
- Az incidenssel érintett igazgatási/szervezeti egység megnevezése és elérhetőségei
- A bejelentő adatkezelő címe és egyéb elérhetőségei
- A bejelentő természetes személy neve és beosztása
- A bejelentő természetes személy elérhetőségei
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és beosztása
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó e-mail elérhetősége
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó telefonszáma
- Az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó levelezési címe

- Az adatkezelő az alábbiak közül melyik szektorba tartozik

1.2 Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban

- Az adatkezelőn kívül részt vesz-e más személy/szervezet az adatvédelmi incidenssel érintett adatkezelés folyamatában?
- Az adatkezelőn kívüli fél megnevezése és minősége

2. Időpontok

- Adatvédelmi incidens időpontja
- Adatvédelmi incidens kezdő időpontja
- Adatvédelmi incidens záró időpontja
- Az adatvédelmi incidens továbbra is fennáll
- Az incidensről való tudomásszerzés időpontja
- Az incidens észlelésének módja
- Az adatfeldolgozó általi értesítés időpontja
- A késedelmes tájékoztatás indokai
- Egyéb megjegyzések az incidens időpontját érintően

3. Az adatvédelmi incidensről

- Bizalmas jelleg
- Integritás
- Rendelkezésre állás
- Adatvédelmi incidens jellege (több válasz is elfogadható)
- Egyéb megjegyzés az adatvédelmi incidens részletes leírásához
- Adatvédelmi incidens okai (több válasz is elfogadható)
- Adatvédelmi incidens egyéb okainak leírása

4. Az adatvédelmi incidenssel érintett személyes adatok

4.1 Személyes adatok

- Személyazonossághoz kapcsolódó adatok
- Személyi szám
- Elérhetőségi adatok
- Azonosító adatok
- Gazdasági, pénzügyi adatok
- Képfelvétel
- Hangfelvétel
- Hivatalos okmányok
- Helymeghatározó adatok
- Biometrikus adatok
- Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok

4.2 Különleges adatok

- Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok
- Politikai véleményre vonatkozó adatok
- Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok

- Érdekképviseleti szervezeti tagságra vonatkozó adatok
- Szexuális életre vonatkozó adatok
- Egészségügyi adatok
- Genetikai adatok
- Még nem ismert
- Egyéb
- Az egyéb személyes adatok leírása
- Az adatvédelmi incidenssel érintett személyes adatok becsült száma

5. Az érintettek

- Alkalmazottak
- Felhasználók
- Feliratkozók
- Diákok
- Katonai állomány tagjai
- Ügyfelek (jelenlegi és potenciális)
- Páciensek
- Kiskorúak
- Kiszolgáltatott személyek
- Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek
- Még nem ismert
- Egyéb
- Az egyéb leírása
- Az incidenssel érintett adatalanyok részletes leírása
- Az adatvédelmi incidenssel érintettek becsült száma

6. Az incidens ELŐTT alkalmazott intézkedések

- Az adatvédelmi incidens előtt alkalmazott intézkedések leírása

7. Következmények

7.1 Bizalmas jelleg sérülése

- Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult
- Az adat összekapcsolhatóvá vált az érintett egyéb adatával
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges
- Egyéb
- Az egyéb bizalmas jelleget érintő következmény leírása

7.2 Integritás sérülése

- Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt
- Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták
- Egyéb
- Az egyéb integritást érintő következmény leírása

7.3 Rendelkezésre állás sérülése

- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése
- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása
- Egyéb
- Az egyéb rendelkezésre állást érintő következmény leírása

7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények

- Az incidens valószínűsíthető hatásai az érintettekre
- Az egyéb valószínűsíthető hatások leírása
- A valószínűsíthető következmények súlyossága

8. Megtett intézkedések

8.1 Érintettek tájékoztatása

- Érintettek tájékoztatása
- Tájékoztatás időpontja („a" válasz esetén)
- Tájékoztatás tervezett időpontja („b" válasz esetén)
- A tájékoztatás tervezett időpontja még nincs eldöntve („b" válasz esetén)
- Tájékoztatás hiányának indokai („c" válasz esetén)
- Intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor („c" válasz esetén)
- Tájékoztatott érintettek száma („a" válasz esetén)
- Az érintett tájékoztatásának formája („a" válasz esetén)
- Az érintetteknek szóló tájékoztatás tartalma („a" válasz esetén)
- Nyilvánosan közzétett információk, vagy hasonló intézkedés („c" illetve „III" válasz esetén)

8.2 Az adatvédelmi incidens orvoslására tett intézkedések

- Az adatkezelő által az adatvédelmi incidens orvoslására tett intézkedések

8.3 Egyéb bejelentések

- A vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens
- Az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet
  (több válasz is elfogadható)
- Az adatkezelő bejelentette-e, vagy be fogja-e jelenteni az adatvédelmi incidenst közvetlenül más tagállam felügyeleti hatóságának?
- Az EU felügyeleti hatóságok listája, amelyeknek az adatkezelő közvetlenül bejelentette, vagy be fogja jelenteni az adatvédelmi incidenst (több válasz is elfogadható)
- Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst másik EGT-tagállam olyan adatkezelőjének, amely részére az incidenssel érintett adatokat korábban továbbította, vagy amely adatkezelő az incidenssel érintett adatokat részére átadta?
- Azon más EGT-tagállami adatkezelő megnevezése és elérhetőségei, amelynek az incidenst bejelentette vagy be fogja jelenteni.

- Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst EU-n kívüli adatvédelmi hatóságnak?
- Az EU-n kívüli felügyeleti hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette, vagy be fogja jelenteni az adatkezelő
- Bejelentette-e, vagy be fogja-e jelenteni az adatkezelő az adatvédelmi incidenst egyéb EU-s hatóságnak egyéb jogszabály alapján fennálló kötelezettség alapján (NIS Irányelv, eIDAS Rendelet)?
- Egyéb EU hatóságok listája, amelyeknek az adatvédelmi incidenst bejelentette vagy be fogja jelenteni az adatkezelő.

11.10. Kockázatelemzés

A folyamatot támogató, kiszolgáló informatikai rendszerek időszakos leállása, kiesése, működési zavara miatti késedelem vagy kiesés esetei. Lehetséges károk típusai, nagysága, elhárítása. Útmutatás arra, hogy az IT kockázatelemzés eredményei alapján a káresemények, és az általuk okozott károk közül melyeket szükséges figyelembe venni a DR tervek készítése során.

Az adatok és az adott információs rendszer jellegéből kiindulva a kockázatelemzés alapját:

- az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, és az elektronikus információs rendszerelemek sértetlenségének és rendelkezésre állásának sérüléséből, elvesztéséből bekövetkező kár vagy káros hatás, terjedelme, nagysága
- a kár bekövetkezésének vagy a kárral, káros hatással fenyegető veszély mértéke, becsült valószínűsége képezi

Jelölés	Kockázat	Gyakoriság, illetve támadási potenciál
1	kicsi	kb. 5-10 évente előforduló, vagy csak profi támadó által kihasználható gyengeség
2	közepes	éves távlatban előforduló, vagy átlagos szakember által kihasználható gyengeség
3	nagy	évente egyszer előforduló, vagy átlagos szakember által végrehajtható visszaélés

ID	Veszélyforrás	Kár			Bekövetkezés valószínűsége	Kockázat
		C-Bizalmasság	I-Sértetlenség	A-Rendelkezésre állás	V-Valószínűség	R
1	Adatvesztés	1-3	1-3	1-3	1-3	1-81

A kockázatelemzés során figyelembe vett képlet R=H*V (H=CIA szorzat) az így kapott érték skála 1-81 közötti érték között mozoghat. Az intézkedést igénylő kockázati szintet a szervezet 16 fölötti érték jelenti.

12. Adatvédelmi hatásvizsgálat szabályai és elvei

Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja. Az Uniós rendelet három kiemelt esemény bármelyikének megvalósulása esetén kötelezőnek tekinti a hatásvizsgálat elvégzését.

- automatizált döntéshozatali – ideértve a profilalkotási eljárások esetén
- személyes adatok különleges kategóriái (Rendelet 9. cikk), vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok (Rendelet 10. cikk) nagy számban történő kezelése
- nyilvános helyek nagymértékű, módszeres megfigyelése
- ezen túlmenően is hatásvizsgálatot kell végezni minden olyan adatkezelés tekintetében, amelyek valószínűsíthetően magas kockázattal járnak az érintettekre nézve.

12.1. Nem kell az adatvédelmi hatásvizsgálatot elvégezni

- az adatkezelés valószínűsíthetően nem jár magas kockázattal,
- egymáshoz hasonló típusú adatkezelési műveletek esetében, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat is elegendő, azaz nem kell feltétlenül külön hatásvizsgálatot készíteni (GDPR, 35. cikk (1) bekezdés),
- a 6. cikk (1) bekezdésének c) vagy e) pontja szerinti adatkezelés (az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges) jogalapját **uniós vagy az adatkezelőre alkalmazandó tagállami jog írja elő, és e jog a szóban forgó konkrét adatkezelési műveletet vagy műveleteket is szabályozza**, valamint e jogalap elfogadása során **egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot** (GDPR, 35. cikk (10) bekezdés),
- a felügyeleti hatóság **azon listáján szerepel, amely szerint az adott kezelés tekintetében nem kötelező hatásvizsgálatot végezni** (lásd az előző pontban írtakat is).

12.2. Kötelező az adatvédelmi hatásvizsgálatot elvégezni

Ha a Szervezet alkalmaz profilalkotó eljárásokat, kezel különleges kategóriájú személyes adatokat, foglalkozik közterület szisztematikus megfigyelésével. Új szolgáltatások bevezetése vagy az adatkezelést előíró jogszabályi környezet megváltozása esetén meg kell vizsgálni, hogy a megváltozott adatkezelés indokolja e az adatvédelmi hatásvizsgálat elvégzését.

Az adatvédelmi hatásvizsgálat megkezdését az ügyvezető hagyja jóvá az adatvédelmi felelős vagy tisztviselő javaslatát figyelembe véve.
A kötelező esetkörökön kívül az ügyvezető elrendelheti bármely adat kezelésére vonatkozóan hatásvizsgálat elvégzését, amennyiben az adatkezelés a kockázati besorolás alapján magas kockázatúnak minősül.

Az adatkezelés magas kockázatúnak minősül, ha az alábbi kockázati tényezők közül legalább három azonosításra került:

<table>
<tr><th>Adatkezelés ismérvei</th><th>Kockázatkeletkező tényező</th></tr>
<tr><td>Adatkezelés jellege</td><td>
<table>
<tr><th>Tényező</th><th>Megvalósul</th></tr>
<tr><td>Az adatkezelésből:
- hátrányos megkülönböztetés,
- személyazonosság-lopás vagy személyazonossággal való visszaélés,
- pénzügyi veszteség,
- a jó hírnév sérelme,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése,
- az álnevesítés engedély nélkül történő feloldása,
- bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat.</td><td><u>Igen / Nem</u></td></tr>
</table>
</td></tr>
<tr><td>Adatkezelés hatóköre</td><td>
<table>
<tr><th>Tényező</th><th>Megvalósul</th></tr>
<tr><td>Olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>A kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Az adatkezelés nagy mennyiségű (kevés személyre, de részletes adatokkal) személyes adat alapján zajlik, és nagyszámú (legalább 1000 fő) érintettre terjed ki</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor</td><td><u>Igen / Nem</u></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Adatkezelés körülményei</td><td>
<table>
<tr><th>Tényező</th><th>Megvalósul</th></tr>
<tr><td>Az érintettek nem gyakorolhatják jogaikat és szabadságaikat</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Az érintettek nem rendelkezhetnek saját személyes adataik felett.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Automatizált döntéshozatal épül az adatkezelésre.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Az érintett módszeres megfigyelését igényli az adatkezelés.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Kiszolgáltatott helyzetben lévő érintettre vonatkozik az adatkezelés.</td><td><u>Igen / Nem</u></td></tr>
<tr><td>Az alkalmazott technológia új, innovatív, amellyel az érintettek még nem találkozhattak.</td><td><u>Igen / Nem</u></td></tr>
</table>
</td></tr>
<tr><td>Adatkezelés célja</td><td>
<table>
<tr><th>Tényező</th><th>Megvalósul</th></tr>
<tr><td>Személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából.</td><td><u>Igen / Nem</u></td></tr>
</table>
</td></tr>
</table>

A hatásvizsgálat elvégzésére vonatkozó javaslatot az adatvédelmi tisztviselő vagy adatvédelmi felelős adja át a szervezet első számú vezetője számára jóváhagyási célból.

Amennyiben a hatásvizsgálat nem kötelező:

- az adatvédelmi felelős választja ki a hatásvizsgálattal érintett adatkezelést, erre vonatkozóan az egyes szervezeti egységek vezetői javaslattal élhetnek az adatvédelmi felelős felé,
- az adatvédelmi felelős a hatásvizsgálat elvégzésére vonatkozó javaslatot a szervezet vezetője számára jóváhagyási célból átadja,
- az ügyvezető a döntés előkészítés során kikéri az adott terület szakmai vezetőjének véleményét, javaslatát a hatásvizsgálat elvégzésére vonatkozóan.

12.3. Feladatok a hatásvizsgálat elvégzése során

A hatásvizsgálat elvégzése során az adatvédelmi tisztviselő:

- a hatásvizsgálatot dokumentálja,
- azonosítja a kockázatokat (figyelembe véve az elérhető nemzetközi és hazai gyakorlatot, valamint a 29-es munkacsoport ajánlásait),
- az azonosított kockázatok kezelésére javaslatot tesz,

- dokumentálja a kockázatok kezelésére tett javaslatokat,
- ellenőrzi a javaslatok megvalósítását.

A hatásvizsgálat elvégzése során a hatásvizsgálatban vizsgált adatkezelést megvalósító szervezeti egységek az adatvédelmi tisztviselő felhívására:

- 10 napon belül adatot szolgáltatnak,
- közreműködnek a javaslatok megvalósításában.

A hatásvizsgálat elvégzése során az informatikai terület irányítója az adatvédelmi tisztviselő felhívására:

- 10 napon belül adatot szolgáltat,
- közreműködik az informatikai megvalósítást igénylő javaslatok megvalósításában.

Az adatvédelmi tisztviselő:

- közreműködik a hatásvizsgálat elvégzésében a vonatkozó jóváhagyási javaslat előkészítésében,
- a kockázatok azonosításában és a kockázatok kezelésre vonatkozó javaslatok kidolgozásában.

A hatásvizsgálat eredményét a szervezet első számú vezetője hagyja jóvá.

12.4. Feladatok a hatásvizsgálat elvégzését követően

Amennyiben a hatásvizsgálat eredménye azt mutatja, hogy bizonyos kockázatokat nem lehet kezelni, vagy a kezelésre vonatkozó javaslat a kockázatot nem kezeli teljes mértékben, és a kockázatok magas mértékűnek számítanak, az adatvédelmi tisztviselő, a felügyeleti hatósághoz fordul előzetes konzultáció keretében.

Magas kockázatúnak minősül az adatkezelés, ha a hatásvizsgálat alapján megállapított javaslatok megvalósítását követően is fennállnak a kockázatok, vagy, ha továbbra is az állapítható meg, hogy a kockázatok kezelését követően is az érintettek magánszférája, jogai nagy valószínűséggel sérülhetnek az adatkezelés miatt.

A felügyeleti hatósághoz fordulást a hatásvizsgálatot jóváhagyó személy engedélyezi.

13. Adatbiztonsági előírások

Az információ- és adatvagyon-biztonsági előírások az elektronikus adatkezelés következtében nagyon komoly mélységben kapcsolódnak az informatikai rendszerek és azok üzemeltetésének biztonságához. A személyes adatok védelme részét képezi az adatkezelő teljes adatvagyonának. Mivel az a szabályzat kimondottan a személyes adatok biztonságos kezelésére irányuló tevékenységet szabályozza, így az átfogó információbiztonsági intézkedéseket az IBSZ (Informatikai Biztonsági Szabályzat) tartalmazza, amely előírása a teljes adatvagyonra nézve kötelező jellegűek, ezért ennek a területnek a szabályozása ezen dokumentumnak nem része. Viszont az adatvédelmi és adatkezelési szabályzat tartalmazza azokat a fontosnak tekintett főbb folyamatokat, amelyek részletes szabályozása az IBSZ-ben megtekinthetőek.

13.1. Fizikai és környezeti biztonság

A fizikai és környezeti biztonsági intézkedéseknek alkalmasnak kell lenniük a lopásból, jogosulatlan hozzáférésből, hőmérsékletből, tűzből, füstből, vízből, rázkódásból, terrorcselekményekből, vandalizmusból, áramkimaradásból, kémiai

anyagokból vagy robbanószerekből eredő kockázatok hatékony megelőzésére, feltárására és csökkentésére.

A fizikai behatások pénzügyi veszteséghez, jogi következményekhez, hitelvesztéshez vagy versenyelőny elvesztéséhez vezethetnek. Ezeket elsődlegesen természeti események vagy emberi közrehatás okozza és eredményük lehet az, hogy az üzletmenethez jogosulatlanul is hozzá lehet férni, vagy hogy az üzleti információk elérhetetlenek lesznek.

A fizikai hozzáférési problémák jelentős veszélyforrások az információbiztonságon belül.

Az okokra és lehetséges elkövetőkre példák:

- jogosulatlan belépés
- berendezések vagy dokumentumok károsítása, vandalizmus vagy lopás
- érzékeny vagy szerzői jogi védelem alatt álló információk másolása vagy megtekintése
- érzékeny berendezések és információk módosítása
- érzékeny információk nyilvánosságra hozása
- adatkezelési erőforrásokkal való visszaélés

A lehetséges elkövetők:

- korábbi munkavállalók
- érdekelt vagy tájékozott külső személyek, mint pl. versenytársak, tolvajok, szervezett bűnözés és hackerek
- egyéb gondatlan munkavállalói magatartás

Információbiztonsági nézőpontból a következő létesítmények védendők, többek között:

- számítógéptermek
- telekommunikációs berendezések
- áramforrások
- mobil eszközök
- helyszíni és távoli nyomtatók
- helyi hálózatok

Továbbá a rendszerek, az infrastruktúra és szoftveralkalmazások dokumentációját védeni kell a jogosulatlan hozzáférés ellen. Ahhoz, hogy ezen védelmi intézkedések hatásosak legyenek, túl kell nyúlniuk a számítógépes környezeten, hogy magában foglalják a sebezhető hozzáférési pontokat és a szervezeti határokat/ interfészeket, ahol a külső hálózatokhoz kapcsolódnak a rendszerek.

13.2. Az IBSZ – szabályozott intézkedések a megfelelőség érdekében

13.2.1. Jelszóképzési és -használati szabályok

A jelszavak fontos részét képezik a számítógépes biztonságnak. Egy nem megfelelően kiválasztott jelszó jogosulatlan hozzáférést és/ vagy az erőforrások jogosulatlan kihasználását eredményezheti. Minden felhasználó saját maga felel a jelszó kiválasztásáért és biztonságos kezeléséért.

13.2.2. Távoli hozzáférési szabályok

Számos felhasználónak, mint pl. a saját munkavállalóknak, külső tanácsadóknak és beszállítóknak szükségük lehet távoli hozzáférésre. Ezen lehetőség biztosításához erre vonatkozó szabályzatoknak és ellenőrző mechanizmusoknak kell létezniük, hogy kielégítsék az üzleti igényeket, csakúgy, mint a biztonsági követelményeket.

A hálózatokhoz és erőforrásokhoz való külső hozzáférést az IBSZ szabályozza és az alábbi 3 mód elfogadható a szervezet számára:

- Távoli hozzáférés (SSL VPN)
- Site-to-Site VPN
- TeamViewer és az ahhoz hasonló rendszerek

Az adatokhoz vagy rendszerekhez való távoli hozzáférést a lehetséges minimum szinten kell tartani a szükség szerinti hozzáférés elvének bevezetésével.

13.2.3. Malware védelem

A malware (az ártalmas szoftver [malicious software] angol szavak rövidítéséből) fogalmát általában széles körben használják a kártékony számítógépes programokra, mint pl. vírusok, kémprogramok, férgek, trójai programok, rootkitek, stb., amelyeket olyan rosszhiszemű szándékkal hoztak létre, hogy károsítsa a számítógépes rendszereket.

Az ártalmas szoftverek és az eszközök ártalmas felhasználása ellen az alapvető biztonsági intézkedéseket az IBSZ tartalmazza, melyet minden informatikai eszközt használó vagy a szervezet informatikai hálózatához csatlakozó személynek be kell tartania.

13.2.4. Javításkezelés

A javításkezelés a rendszerkezelés olyan területe, amely magában foglalja a javítások (patch-ek) beszerzését, tesztelését és telepítését a kezelt számítógépes rendszeren, annak érdekében, hogy naprakész szoftverek fussanak, illetve gyakran a biztonsági kockázatok kezelése érdekében.

A javításkezelési feladatok magukban foglalják a következőket:

- Minden rendszer elérhető javításairól való tudomásszerzés
- Annak meghatározása, hogy milyen javítások szükségesek bizonyos rendszerekhez
- Annak biztosítása, hogy a javításokat megfelelően tesztelik a bevezetés előtt
- Javításkezelési eljárások dokumentálása

A hálózat felhasználásából, újra indulásából és/ vagy a rendszer erőforrások szükségtelen használatából eredő üzletmenet megszakadás minimalizálása érdekében csak a kritikus vagy biztonsággal kapcsolatos javításokat kell alkalmazni.
Részletes szabályozást az IBSZ tartalmazza

13.2.5. Mobil adathordozók kezelése és szállítása, megsemmisítése

Megfelelő ellenőrző mechanizmusokat kell alkalmazni, hogy megelőzzük a számítógépeken, lemezeken és más berendezésen vagy adathordozókon tárolt érzékeny információhoz való hozzáférést vagy ezek elvesztését (pl. papíralapú

dokumentumok, meghajtók, USB memóriák, CD/DVD stb.), hogy megelőzhető legyen a belső, bizalmas vagy korlátozott hozzáférésű információk nyilvánosságra kerülése. Részletes szabályozást az IBSZ tartalmazza.

13.2.6. Fájltovábbítási szabályok

Az érzékeny adatokat tartalmazó céges fájlok vagy megbízói fájlok megosztása nem biztonságos kommunikációs csatornákon nagy biztonsági kockázatot jelent. Amikor fájlküldésről van szó, az érzékeny adatok biztonsága elsődleges prioritást élvez és SFTP-t és FTPS-t kell használni FTP helyett.

A személyes adatokat tartalmazó dokumentumok szervezeten belüli továbbításra az elektronikus levelező rendszer nem, vagy csak korlátozott módon használható. Az e-mailen küldött érzékeny adatokat tartalmazó csatolmányok megnyitás elleni védelméről minden munkavállalónak gondoskodnia kell.
Részletes szabályozást az IBSZ tartalmazza.

13.2.7. Biztonsági mentés szabályai

A biztonsági mentés szabályzat célja annak biztosítása, hogy az adatok ne vesszenek el és helyreállíthatók legyenek berendezéshiba, szándékos vagy véletlen rongálódás/ adatvesztés vagy katasztrófa esetén. Egyedi ellenőrző mechanizmusokat kell használni, hogy az adatbiztonsági mentések és helyreállítás kezelésével kapcsolatos kockázatok csökkenjenek.

- Minden éles és kritikus rendszert és adatot, amelyek fontosak a folyamatos működéséhez, teljes egészében biztonsági mentéssel kell biztosítani legalább napi szinten.
- A biztonsági mentést úgy kell végezni, hogy az biztosítsa, hogy az adatok rendszerhiba esetén is helyreállíthatók legyenek.
- Azonnali teljes adatbiztonsági mentést kell készíteni, amikor nagymértékben változnak az adatok, vagy nagymértékű javítási csomag-, vagy szoftver verzió váltásra kerül sor.
- A fontos adatokat napi kumulatív (csak a változó adatokat rögzítő) biztonsági mentésekkel, illetve heti teljes biztonsági mentéssel is biztosítani kell.
- A részleges rendszer helyreállításokat, kiválasztott fájlcsoportok szúrópróbaszerű helyreállításával rendszeresen el kell végezni az Incidenskezelési folyamat részeként.

A helyreállítási eljárásokat rendszeresen ellenőrizni és tesztelni kell (legalább évente) annak biztosítása érdekében, hogy hatékonyak és a helyreállításra előírt eljárásokban meghatározott idő alatt elvégezhetők legyenek. A biztonsági mentések szakmai szabályait és körülményeit az IBSZ tartalmazza.

14. Hatálybalépés

Ez a szabályzat az címlapon meghatározott napon lép hatályba. A Szervezet vezetője a szabályzatot haladéktalanul, de legfeljebb 15 napon belül – a hatálybalépés naptári napjának feltüntetésével – közzéteszi a Szervezeten beül mindenki számára elérhető módon. Az adatvédelemmel összefüggő szabályzatok, nyilvántartások elfogadását követően – a hatályba léptetést megelőzően – a Szervezet szabályzatokban,

nyilvántartásokban érintett munkavállalói számára, oktatás keretében kerülnek megismertetésre. Az adatkezelési szabályzat publikus részéből az Adatkezelő tájékoztatót készít, amit többek között a weboldalán is megjelentet. Az adatvédelemmel összefüggő szabályzatok, nyilvántartások, tájékoztatók, érdekmérlegelési tesztek elfogadásukat követően, évente kerülnek felülvizsgálatra. A felülvizsgálat befejezését követően tudatosságnövelő tréning keretében kerül ismertetésre a dokumentációban átvezetésre kerülő változás.

Budapest, 2024. szeptember 1.

Devich Gábor
ügyvezető

Concerto Akadémia Nonprofit Kft 1094 Budapest, Páva u. 10-12. Adószám: 18312777-2-43