FŐVÁROSI VÍZMŰVEK

Adatfeldolgozási tevékenység végzésére vonatkozó előírások

Jelen „Adatfeldolgozási tevékenység végzésére vonatkozó előírások" (a továbbiakban mint az „Előírások") határozza meg a Fővárosi Vízművek Zártkörűen Működő Részvénytársasággal mint megrendelővel, illetve megbízóval (a továbbiakban mint az „Adatkezelő") vállalkozási, illetve megbízási szerződést (a továbbiakban mint a „Szerződés") kötő vállalkozó, illetve megbízott (a továbbiakban mint az „Adatfeldolgozó") számára a Szerződés teljesítésével összefüggésben Adatkezelő nevében végzett személyes adatok kezelésének és az adatfeldolgozási tevékenység végzésének alapvető feltételeit, valamint az Adatkezelő és az Adatfeldolgozó között keletkező adatfeldolgozási jogviszonyból eredő jogokat és kötelezettségeket.
Az Előírások alapját a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló az Európai Parlament és a Tanács (EU) 2016/679 rendelete (a továbbiakban mint a „GDPR"), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban mint az„Infotv.") képezik, melyek rendelkezései az Adatkezelő javára végzett valamennyi adatfeldolgozási tevékenység kapcsán minden esetben irányadók. Az Előírásokban nem definiált fogalmak a fenti jogszabályokban meghatározott jelentésnek megfelelően értelmezendőek. Eltérő rendelkezés hiányában, a Szerződésben, illetve a Szerződésben foglalt speciális elvárások és utasítások tekintendőek irányadónak az Előírásokban foglalt minimum követelményekkel szemben.

1. Az adatkezelés céljának meghatározása. Az Adatkezelő azon személyes adatok kezelése tekintetében, amelyeket az Adatfeldolgozó részére továbbít, megfelelő jogalappal rendelkezik, és azokat a Szerződésben meghatározottak teljesülése érdekében jogosult az Adatfeldolgozó részére átadni. Az Adatfeldolgozó a személyes adatokat saját céljára nem használhatja fel, azokat az Előírásokban foglaltak szerint, és csak a Szerződésben foglaltak teljesítéséhez szükséges mértékben és ideig kezelheti.

2. Jogok és kötelezettségek. Az Adatfeldolgozó a személyes adatokat a Szerződés teljesítése érdekében, az Adatkezelő utasításai szerint kezeli, kivéve, ha az adatkezelést jogszabály írja elő.
Az Adatfeldolgozó szavatolja, hogy a jogszabályokban rögzített kötelezettségeket, kiemelten a GDPR. 28. cikkében megfogalmazott rendelkezéseket, a Szerződés tartama alatt maradéktalanul betartja. Az Adatfeldolgozó továbbá szavatolja, hogy adatkezelési tevékenysége a jogszabályokban foglalt követelményeknek maradéktalanul megfelel, és vállalja, hogy az érintettek jogainak és szabadságainak védelmét biztosító, megfelelő technikai és szervezési intézkedéseket végrehajtja. Az Adatfeldolgozó szavatolja, hogy az Adatkezelő rendelkezésére bocsát minden olyan információt, amely a GDPR 28. cikkében meghatározott kötelezettségeinek teljesítésének igazolásához szükséges, továbbá minden olyan információt is köteles az Adatkezelő rendelkezésére bocsátani, amely lehetővé teszi és elősegíti az Adatkezelő által vagy általa megbízott más ellenőr által végzett auditokat. Az Adatfeldolgozó vállalja, hogy a hozzá esetlegesen benyújtásra került adatvédelmi tárgyú kérelmet haladéktalanul, legkésőbb 7 (hét) napon belül továbbítja az Adatkezelő részére. Az Adatfeldolgozó segíti az Adatkezelőt abban, hogy teljesüljenek az adatvédelmi hatásvizsgálat elvégzéséből és a felügyeleti hatósággal folytatott konzultációkból eredő kötelezettségek, amelyekért díjat, illetve költséget nem számíthat.

3. További Adatfeldolgozók igénybevétele. Az Adatfeldolgozó az Adatkezelő előzetes írásban tett eseti vagy általános felhatalmazása nélkül további Adatfeldolgozót (a továbbiakban mint az „Al-adatfeldolgozó") nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az Adatfeldolgozó tájékoztatja az Adatkezelőt megfelelő időn belül minden olyan tervezett változásról, amely további Al-adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva a lehetőséget az Adatkezelőnek arra, hogy ezekkel a változásokkal szemben kifogást emeljen. Az Adatfeldolgozó és az Al-adatfeldolgozó közötti megállapodásnak ugyanazon adatvédelmi kötelezettséget kell tartalmaznia, mint amelyek az Adatkezelő és az Adatfeldolgozó között létrejöttek, így különösen:
(a) az Al-adatfeldolgozónak megfelelő garanciákat kell nyújtania arra vonatkozóan, hogy megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy az adatfeldolgozás megfeleljen az adatvédelmi jogszabályban foglaltaknak, továbbá
(b) az Al-adatfeldolgozó köteles eleget tenni az Előírásokban foglaltaknak.
Az Al-adatfeldolgozó adatvédelmi kötelezettségeinek megszegéséért az őt megbízó Adatfeldolgozó teljes felelősséggel tartozik az Adatkezelő irányába, amelyre vonatkozóan az Előírások 10. pontjában leírtak irányadóak. Harmadik országban történő adatfeldolgozásra, adattovábbításra az Adatkezelő és az Adatfeldolgozó külön írásbeli megállapodása esetén kerülhet sor.

4. Az adatfeldolgozás biztonsága. Az Adatfeldolgozó köteles a személyes adatok feldolgozásának teljes életciklusában megvalósítani és biztosítani a személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását, valamint köteles megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Az Adatfeldolgozónak kötelessége továbbá a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének, integritásának, rendelkezésre állásának és ellenálló képességének biztosítása a Szerződés teljes időszaka alatt.

5. Adminisztratív védelem. Az Adatfeldolgozó a személyes adatok védelme céljából alkalmazott információbiztonság biztosítása érdekében, köteles az ügyviteli gyakorlatba ültetett és bevezetett szabályzattal vagy szabályzatokkal rendelkezni, valamint azok betartását szavatolni. Az Adatfeldolgozó köteles dokumentálni az adatvédelmi követelmények teljesítése érdekében általa alkalmazott műszaki biztonsági és szervezetbiztonsági intézkedéseket. A dokumentációt (legyen az szabályzat, eljárásrend, vagy technikai leírás) igény esetén az Adatkezelő rendelkezésére kell bocsátani. Amennyiben az Adatfeldolgozó tudomást szerez arról, hogy akár a saját, akár valamely Al-adatfeldolgozójának szervezete nem felel meg az Előírásokban foglalt biztonsági intézkedéseknek, az adott meg nem felelést köteles haladéktalanul bejelenteni az Adatkezelőnek.

6. Fizikai védelem. Az Adatfeldolgozó köteles a személyes adatok feldolgozásában részt vevő hardver komponensek és azoknak helyt adó helyiségek fizikai védelmét biztosítani, illetve minden olyan területen is biztosítani, ahol az Adatfeldolgozó olyan feladatokat végez az Adatkezelő részére, amelyek potenciálisan kihathatnak az Adatkezelő személyes adataira. Mechanikai-, és elektronikai védelmet szükséges biztosítani (a kockázatokkal arányos módon) annak érdekében, hogy a személyes adatokat tartalmazó vagy feldolgozó hardver elemekhez (például, de nem kizárólag: személyi számítógép, laptop, külső és belső merevlemez, szerver számítógép, központi adattároló, switch, router, kábelhálózat stb.) csak az adatfeldolgozásban részt vevő személy férhessen hozzá. Az Adatfeldolgozó szavatol azért, hogy a fizikai biztonsági szabályait minden területen alkalmazzák, ahol az Adatfeldolgozó vagy az Al-adatfeldolgozó az Adatkezelő részére végez feladatokat, oly módon, hogy az így elért fizikai védettség folyamatosan – a mindenkori technológiai fejlődést követve – is biztosítva legyen.

7. Logikai védelem. Az Adatfeldolgozó a biztonság folyamatos érvényesülése érdekében köteles az alábbiakat biztosítani:
(a) az üzemeltetéssel kapcsolatos biztonsági rések kezelésére vonatkozó irányítási eljárásrendet kialakítani, azzal a céllal, hogy felderítse, és ezt követően kellő időben, biztonsági javítások alkalmazásával vagy a kockázat egyéb mérséklése révén megszüntesse vagy semlegesítse az összes ismert sebezhetőséget;
(b) rosszindulatú programok elleni védelmet (antimalware) telepíteni az összes felhasznált olyan végpontra, amelyen a rosszindulatú program elleni védekezés releváns, ideértve az anti-malware szoftver folyamatos frissítési mechanizmusát is;
(c) tűzfal megoldást telepíteni az összes felhasznált végpontra;
(d) módszeresen megerősíteni a rendszereit, hogy minimálisra szorítsa azok támadható felületét;

(e) mechanizmusokat alkalmazni a releváns adatok összes számítógépről történő központosított biztonsági mentése, valamint bármilyen központi tárhely biztonsági mentése érdekében;
(f) megoldásokat alkalmazni úgy az összes naplóadatainak (hálózati eszközökről az operációs rendszer útján és az adatbázisokból alkalmazásokkal történő), mint forgalmi (adatcsere) adatainak gyűjtésére és elemzésére a teljes infrastruktúrájából, valamint folyamatosan proaktívan figyelemmel kísérni az elemzési eredményeket azzal a céllal, hogy a gyanús vagy anomáliát jelentő megfigyeléseket kimutassa, azokra reagálni tudjon;
(g) biztonsági mechanizmusokat alkalmazni a hálózati forgalom megfigyelése tekintetében, hogy a rosszindulatú tevékenységeket és potenciális támadásokat felderítse és megakadályozza; és
(h) az Adatkezelő felhívása és ésszerű előzetes értesítése esetén az Adatkezelő rendelkezésére bocsátani az Adatfeldolgozó által abból a célból bevezetett intézkedésekkel kapcsolatos információkat, hogy fellépjen a rosszindulatú programkód az Adatfeldolgozó környezetébe (környezeteibe) vagy olyan környezetekbe történő bevezetése ellen, amelyeket az Adatkezelő rendszereinek vagy infrastruktúrájának távoli eléréséhez vesznek igénybe. Az adatokat kötelező védeni a használaton kívüli és elveszett eszközök esetében is.

8. Hozzáférések kezelése. A személyes adatok feldolgozásával kapcsolatos feladatok személyekhez rendelése során kötelezően érvényesíteni kell a feladatok szigorú elkülönítését. A hozzáférési jogokat, jogosultságokat és tevékenységeket kezelő, kiosztó vagy felügyelő bármely rendszerben vagy mechanizmusban (műszaki vagy irányítási értelemben) a felelősségi és feladatkörök személyekhez rendelésének úgy kell történnie, hogy egyetlen személynek se legyen lehetősége a saját hozzáférési jogai, jogosultságai és tevékenységei kezelésére, kiosztására vagy felügyeletének befolyásolására, emellett magában a rendszerben is szükségesek olyan ellenőrzések és korlátozások, amelyek megakadályozzák ennek véletlenszerű vagy szándékos előfordulását. Az Adatkezelő adataihoz történő hozzáférés minimálisra szorítása érdekében a legkisebb körű hozzáférés és legkevesebb jogosultság elveit kell alkalmazni.
Az Adatfeldolgozó hozzáférés-kezelési folyamata eleget kell, hogy tegyen az alábbiaknak:
(a) a rendszerekhez és információkhoz kizárólag illetékes személyek, azaz olyanok férhetnek hozzá, akik az Adatkezelő részére végeznek munkát, minden folyamatnak tényleges igényeken kell alapulnia;
(b) az Adatfeldolgozó az Adatkezelő felhívására köteles késedelem nélkül az Adatkezelő rendelkezésére bocsátani az Adatfeldolgozónál bevezetett hozzáférés-ellenőrzési mechanizmusokra, és naplózással megvalósított nyomon-követhetőségi eljárásrendekre vonatkozó információkat; továbbá
(c) az Adatfeldolgozó az Adatkezelő rendszereivel és személyes adataival munkát végző összes munkatársa hozzáférési jogainak rendszeres, minimum évenkénti felülvizsgálatára köteles.

9. Titoktartás. A Szerződésben meghatározott titoktartási kötelezettségen túl az Adatkezelő az alábbi adat- és titokvédelmi előírások betartására is köteles:
(a) az Adatfeldolgozó köteles biztosítani, hogy a személyes adatok feldolgozásába általa bevont személyek (pl. tisztségviselők, munkavállalók, szaktanácsadók, alvállalkozók és egyéb közreműködők, az Al-adatfeldolgozókat és azok személyzetét is ideértve) titoktartási kötelezettséget vállaljanak;
(b) az Adatfeldolgozó köteles megtenni azokat a technikai és szervezési intézkedéseket, valamint kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek;
(c) az Adatfeldolgozó az általa az Adatkezelő nevében feldolgozott személyes adatokat köteles az Adatkezelő bármikori felhívására (vagy a Szerződésben rögzített megőrzési idő eltelte után külön értesítés hiányában is) késedelem nélkül, az Adatkezelő utasítása szerint véglegesen törölni vagy azokat visszajuttatni az Adatkezelő részére, kivéve, ha európai uniós vagy magyar jogszabály a személyes adatok tárolását írja elő részére; valamint
(d) az Adatfeldolgozó az Adatkezelő részére kezelt személyes adatokat tartalmazó iratokról, dokumentumokról másolatot, kivonatot kizárólag az Adatkezelő írásbeli előzetese engedélye alapján készíthet.
Egyebekben a személyes adatok feldolgozásához kapcsolódó titoktartási kötelezettségre a Szerződésben meghatározott rendelkezések irányadóak.

10. Incidensek kezelése. Az Adatfeldolgozó kötelezettséget vállal arra, hogy amennyiben tudomására jut valamely, az Adatkezelő által részére átadott személyes adatokkal kapcsolatos adatvédelmi incidens, arról az Adatkezelőt kapcsolattartója útján indokolatlan késedelem nélkül, de legfeljebb 24 (huszonnégy) órán belül értesíti. Az Adatfeldolgozó indokolatlan késedelem nélkül köteles minden ésszerű lépést megtenni, és minden indokolt intézkedést bevezetni annak érdekében, hogy minimalizálja az adatvédelmi incidensek miatti negatív hatásokat. Az Adatfeldolgozó az értesítésében, amennyiben ezen információk a 24 órás határidőn belül rendelkezésre állnak, köteles információt adni az Adatkezelő felé az alábbiakról:
(a) az incidens bekövetkezésének időpontja (kezdete és vége) és a tudomásszerzés időpontja;
(b) az incidens körülményei, oka, és következményei;
(c) az incidens során érintettek személye és (becsült) száma, az érintett adatok köre, jellege és száma; és
(d) az incidens súlyossága és az elhárítása érdekében tett vagy tervezett intézkedések.
Az Adatfeldolgozó köteles az Adatkezelő kérésére a belső incidens nyilvántartása másolatának az Adatkezelő tekintetében releváns részét a rendelkezésre bocsátani. A késedelmes értesítésből, illetőleg intézkedésből eredő károkért az Adatfeldolgozó teljes felelősséggel tartozik az Adatkezelő felé.

11. Audit és ellenőrzés. Az Adatkezelő az adatvédelemmel, illetve az Előírásokban foglaltakkal összefüggésben auditokat, tesztelést és ellenőrzéseket hajthat végre, amelyekhez az Adatfeldolgozó köteles megadni az indokolt segítséget, és az audit célja szerinti végeredményt alátámasztó dokumentációt, illetve indokolt esetben a helyszíni betekintést biztosítani. Az Adatkezelő harmadik felet is megbízhat azzal, hogy az Adatkezelő számára segítséget nyújtson az auditok, tesztelés és ellenőrzések végrehajtásában, vagy azokat az Adatkezelő nevében végrehajtsa. Az ilyen tárgyú auditok, tesztek és ellenőrzések 12 (tizenkettő) havonta egy alkalommal végezhetők, kivéve, ha a megelőző 12 (tizenkettő) hónapban végrehajtott audit, tesztelés vagy ellenőrzés olyan súlyos megállapításokat eredményezett, amelyek ésszerűen indokolttá teszik az utóellenőrzés vagy kiterjesztett terjedelmű audit végrehajtását, így különösen, de nem kizárólag, ha:
(a) az Adatkezelőt, a személyes adatokat vagy az Adatfeldolgozó jelen melléklet szerinti kötelezettségei teljesítésével kapcsolatos képességét lényegesen érintő súlyos biztonsági esemény (pl. adatvédelmi incidens) következett be, vagy ez megalapozottan várható, ami ésszerűen indokolttá teszi a kapcsolódó technológiai-, szervezeti-, szabályzati hatókör auditálását;
(b) az Adatkezelő és az Adatfeldolgozó által közösen megállapított adatvédelmi és biztonsági szabályzatok megsértésére került sor, vagy ez megalapozottan várható, ami ésszerűen indokolttá teszi a kapcsolódó technológiai-, szervezeti-, szabályzati hatókör auditálását;
(c) vagy amennyiben az Adatkezelő megítélése szerint a soron kívüli audit, tesztelés, illetve az ellenőrzés végrehajtását a hazai és/vagy az európai adatvédelmi joggyakorlat fejlődése indokolttá teszi.
Az Adatkezelő köteles legkevesebb 2 (kettő) héttel korábban értesíteni az Adatfeldolgozót az ilyen auditokról, tesztelésről és ellenőrzésekről, kivéve, ha ez hátrányosan befolyásolja a kérdéses audit, tesztelés és/vagy ellenőrzés célját vagy kimenetelét. Ettől függetlenül az előzetes értesítést minden esetben, legkevesebb 24 (huszonnégy) órával korábban biztosítani kell. Az Adatfeldolgozó nem mentesül a felelősség alól, amennyiben az Adatkezelő által végzendő audit nem kerül megindításra. Az Adatfeldolgozó vállalja, hogy a saját költségén késedelem nélkül elhárít az Adatkezelő által feltárt, és az Adatfeldolgozó felé jelzett minden adatvédelemmel és adatbiztonsággal kapcsolatos hiányosságot, problémát. Amennyiben az Adatfeldolgozó nem tesz eleget a Szerződésben vagy az Előírásokban rögzített kötelezettségeinek, az Adatkezelő – az egyéb jogkövetkezmények alkalmazásán túl – a mulasztás orvoslásáig felfüggesztheti a személyes adatok továbbítását az Adatfeldolgozó felé.

12. Felelősség. Az Adatfeldolgozó a Szerződés tartalmával összefüggésben az Adatkezelő részére végzett személyes adatok kezelése keretében felelős a személyes adatokon végzett műveletek jogszerűségéért, továbbá felelősséggel tartozik az adatkezelési tevékenysége által okozott károkért, különösen, ha nem tartotta be a jogszabályban meghatározott kötelezettségeit, vagy ha az Adatkezelő utasításait figyelmen kívül hagyva, vagy azokkal ellentétesen járt el. Amennyiben az Adatfeldolgozó nem az Adatkezelő utasításának megfelelően jár el, az Adatkezelő jogosult a Szerződést felmondani. Az Adatfeldolgozó vállalja, hogy megtérít minden olyan kárt, valamint ezzel összefüggésben felmerült költséget vagy egyéb díjigényt, amely Adatkezelőt az Adatfeldolgozó az Előírásokban meghatározott kötelezettségeinek elmulasztásából vagy azok megszegéséből éri, ide értve minden hatósági, eljárási és ügyvédi költséget is.