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 Adatkezelő javára végzett valamennyi adatfeldolgozási tevékenység kapcsán minden esetben irányadók.

1. Az adatkezelés céljának meghatározása. Adatfeldolgozó a személyes adatokat saját céljára nem használja fel, azokat a jelen mellékletben foglaltak szerint és a Szerződésben foglaltak teljesítéséhez szükséges mértékben kezeli.
Adatkezelő azon személyes adatok kezelése tekintetében, amelyeket Adatfeldolgozó részére továbbít, megfelelő jogalappal rendelkezik, és azokat a Szerződésben meghatározottak teljesülése érdekében jogosult Adatfeldolgozó részére kiadni. Adatkezelő, amennyiben hozzájárulás alapján kezelt személyes adatokat továbbít Adatfeldolgozó részére, úgy az érintetteket megfelelő módon tájékoztatta az adatfeldolgozás tényéről, illetve az Adatfeldolgozó személyéről.

2. Jogok és kötelezettségek. Adatfeldolgozó a személyes adatokat a Szerződés teljesítése érdekében, Adatkezelő utasításai szerint kezeli, kivéve, ha az adatkezelést jogszabály írja elő. Adatfeldolgozó az adatok kezelése céljából nem jogosult további harmadik személyeket, illetve egyéb adatfeldolgozót igénybe venni, kivéve, ha ehhez Adatkezelő írásban előzetesen hozzájárult.
Adatfeldolgozó szavatolja, hogy a jogszabályokban rögzített kötelezettségeket – különösképp a GDPR. 28. cikkében megfogalmazott rendelkezéseket - a Szerződés tartama alatt maradéktalanul betartja.
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. Adatfeldolgozó kijelenti, hogy olyan intézkedéseket alkalmaz, melyekkel az adatkezelési tevékenysége jellegét, hatókörét, körülményeit és céljait és az érintettek adatainak védelméhez fűződő jogát, a megvalósítható intézkedések költségeit is figyelembe véve, megfelelően biztosítható az adatok jogosulatlan vagy véletlenszerű nyilvánosságra hozása, megsemmisítése, megváltoztatása, terjesztése, vagy az ezekhez történő fizikai vagy logikai hozzáférés védelme.
Adatkezelőt és Adatfeldolgozót a személyes adatokra vonatkozóan titoktartási kötelezettség terheli. Adatfeldolgozó köteles megtenni azokat a technikai és szervezési intézkedéseket, valamint kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Adatfeldolgozó az általa Adatkezelő nevében kezelt személyes adatokat a Szerződés teljesülése érdekében, az abból származó igény elévüléséig jogosult kezelni. Ezt követően Adatkezelő döntése alapján Adatfeldolgozó köteles a személyes adatokat törölni vagy visszajuttatni Adatkezelő részére.
Adatfeldolgozó az Adatkezelő részére kezelt személyes adatokat tartalmazó iratokról, dokumentumokról másolatot, kivonatot kizárólag Adatkezelő előzetese engedélye alapján készít. Az engedély alapján kezelt másolatot vagy kivonatot Adatkezelő kérésére Adatfeldolgozó törölni köteles, kivéve, ha uniós vagy magyar jogszabály a személyes adatok tárolását írja elő részére.
Adatfeldolgozó szavatolja, hogy Adatkezelő rendelkezésére bocsát minden olyan információt, amely a GDPR. 28. cikkében meghatározott kötelezettségeinek teljesítésének igazolásához szükséges, továbbá minden olyan információt is köteles Adatkezelő rendelkezésére bocsátani, amely lehetővé teszi és elősegíti Adatkezelő által vagy általa megbízott más ellenőr által végzett auditokat.

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

4. Műszaki és szervezeti biztonsági intézkedések. Adatfeldolgozó köteles a jelen melléklet szerinti kötelezettségeit és intézkedéseit a teljes elvárható szakértelemmel, odafigyeléssel és gondossággal teljesíteni.
Adatfeldolgozó megfelelő műszaki és szervezeti biztonsági és intézkedéseket köteles alkalmazni a személyes adatok bármely illetéktelen vagy jogellenes feldolgozásából, elvesztéséből, megsemmisüléséből, sérüléséből, megváltoztatásából vagy nyilvánosságra kerüléséből származó esetleges károk megelőzése érdekében, figyelemmel a megóvandó személyes adatok jellegére is. Adatfeldolgozó köteles dokumentálni az adatvédelmi követelmények teljesítése érdekében általa alkalmazott műszaki biztonsági és szervezetbiztonsági intézkedéseket. A dokumentációt igény esetén Adatkezelő rendelkezésére kell bocsátani.
Amennyiben Adatfeldolgozó tudomást szerez arról, hogy akár a saját, akár valamely jóváhagyott adatfeldolgozójának / alvállalkozójának szervezete nem felel meg a jelen mellékletben foglalt biztonsági intézkedéseknek, az adott meg nem felelést az adatvédelmi incidensek vonatkozásában rögzített eljárás szerint köteles bejelenteni Adatkezelőnek.

5. Biztonsági audit, tesztelés és ellenőrzés. Adatkezelő a biztonsággal kapcsolatban auditokat, tesztelést és ellenőrzéseket hajthat végre, amelyekhez Adatfeldolgozó köteles megadni az indokolt segítséget és az audit célja szerinti végeredményt alátámasztó dokumentációt.
Adatkezelő egy vagy több általa kiválasztott harmadik felet bízhat meg azzal, hogy Adatkezelő számára segítséget nyújtson a biztonsággal kapcsolatos auditok, tesztelés és ellenőrzések végrehajtásában, vagy azokat Adatkezelő nevében végrehajtsa.
Az egyértelműség kedvéért, az ilyen biztonsági auditoknak, tesztelésnek és ellenőrzéseknek az olyan területekre, rendszerekre és infrastruktúrára kell korlátozódniuk, amelyek potenciálisan befolyásolhatják Adatkezelő biztonságát, a személyes adatokat vagy Adatfeldolgozó képességét jelen melléklet szerinti kötelezettségei teljesítésére. Az ilyen biztonsági auditok, tesztek és ellenőrzések 12 havonta egy alkalommal végezhetők, kivéve, ha a megelőző 12 hónapban végrehajtott biztonsági audit, tesztelés vagy ellenőrzés olyan súlyos megállapításokat eredményezett (pl. műszaki vagy szervezeti jellegű súlyos gyengeségek, biztonsági rések vagy hiányosságok), amelyek ésszerűen indokolttá teszik az utóellenőrzés

vagy kiterjesztett terjedelmű audit végrehajtását, példálózó jelleggel, nem kizárólagosan:
(a) Adatkezelőt, a személyes adatokat vagy Adatfeldolgozó jelen melléklet szerinti kötelezettségei teljesítésével kapcsolatos képességét lényegesen érintő súlyos biztonsági esemény (pl. adatvédelmi incidens) következett be, vagy megalapozottan várható, ami ésszerűen indokolttá teszi a kapcsolódó technológiai és szervezeti hatókör auditálását;
(b) Adatkezelő és Adatfeldolgozó által közösen megállapított biztonsági és adatvédelmi szabályzatok megsértésére került sor, vagy ez megalapozottan várható, ami ésszerűen indokolttá teszi a kapcsolódó technológiai és szervezeti hatókör auditálását.

Adatkezelő köteles legkevesebb két héttel korábban értesíteni Adatfeldolgozót az ilyen auditokról, tesztelésről és ellenőrzésekről, kivéve, ha ez hátrányosan befolyásolja a kérdéses biztonsági audit, tesztelés és/vagy ellenőrzés célját vagy kimenetelét. Ettől függetlenül az előzetes értesítést minden esetben, legkevesebb 24 órával korábban biztosítani kell.
Adatfeldolgozó nem mentesül a felelősség alól, amennyiben Adatkezelő által végzendő audit nem kerül megindításra.

6. Fizikai és környezeti biztonság. Adatfeldolgozó a személyes adatok őrzése céljából alkalmazott fizikai biztonság biztosítása érdekében köteles az ügyviteli gyakorlatba ültetett és bevezetett szabályzattal vagy szabályzatokkal rendelkezni, amit Adatkezelő felhívására és ésszerű értesítése mellett dokumentáltan igazolnia kell.
A személyes adatok megvédésének és őrzésének biztosítása érdekében minden területet, ahol Adatfeldolgozó olyan feladatokat végez Adatkezelő részére, amelyek potenciálisan kihathatnak Adatkezelő személyes adataira, kötelezően biztosítani kell a fizikai biztonsági szabályzatnak vagy szabályzatoknak megfelelően.
Adatfeldolgozó köteles biztosítani, hogy Adatfeldolgozó fizikai biztonsági szabályait minden területen alkalmazzák, ahol Adatfeldolgozó Adatkezelő részére végez feladatokat, oly módon, hogy az így elért fizikai védettség folyamatosan - a mindenkori technológiai fejlődés követve - is biztosítva legyen.
Adatfeldolgozó megfelelő és időszerű biztonsági intézkedések alkalmazásával köteles kellő szintű biztonságot fenntartani a Szerződés teljes időszaka alatt fenntartani az összes olyan végfelhasználói berendezés, szerver, hálózat, digitális adathordozó és mobileszköz vonatkozásában, amelyet Adatkezelőnek nyújtott szolgáltatás céljából használ.
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) hosztgép alapú rosszindulatú programok elleni védelmet (anti-malware) telepíteni az összes felhasznált olyan végpontra, amelyen a rosszindulatú program elleni védekezés releváns, ideértve az anti-malware szoftver folyamatos frissítési mechanizmusát is;
(c) hosztgép alapú 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 node-számítógépről történő központosított biztonsági mentése, valamint bármilyen központi tárhely biztonsági mentése érdekében;
(f) megoldásokat alkalmazni úgy az összes layer 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) Adatkezelő felhívása és ésszerű előzetes értesítése esetén Adatkezelő rendelkezésére bocsátani Adatfeldolgozó által abból a célból bevezetett intézkedésekkel kapcsolatos információkat, hogy fellépjen a rosszindulatú programkód Adatfeldolgozó környezetébe (környezeteibe) vagy olyan környezetekbe történő bevezetése ellen, amelyeket Adatkezelő rendszereinek vagy infrastruktúrájának távoli eléréséhez vesznek igénybe. Az adatokat kötelező védeni a használaton kívüli és elveszett eszközök esetén, adott esetben, igény esetén titkosítási technológia használatával.

7. A feladatok elkülönítése. 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. Adatkezelő adataihoz történő hozzáférés minimálisra szorítása érdekében a legkisebb körű hozzáférés és legkevesebb jogosultság elveit kell alkalmazni.

8. A hozzáférés ellenőrzése. Adatfeldolgozó hozzáférés-kezelési folyamata eleget kell, hogy tegyen az alábbiaknak:
(a) A rendszerekhez és információkhoz kizárólag illetékes személyek, azaz olyanok férhetnek hozzá, akik Adatkezelő részére végeznek munkát. Minden folyamatnak tényleges igényeken kell alapulnia.
(b) Adatfeldolgozó Adatkezelő felhívására és ésszerű előzetes értesítése esetén köteles Adatkezelő rendelkezésére bocsátani az Adatfeldolgozónál bevezetett hozzáférés-ellenőrzési mechanizmusokra és naplózással megvalósított nyomonkövethetőségi eljárásrendekre vonatkozó információkat.
(c) Adatfeldolgozó Adatkezelő rendszereivel és személyes adataival munkát végző összes munkatársa hozzáférési jogainak rendszeres felülvizsgálatára köteles.

9. Incidensek kezelése. Adatfeldolgozó kötelezettséget vállal arra, hogy amennyiben tudomására jut valamely, Adatkezelő által részére átadott személyes adatokkal kapcsolatos adatvédelmi incidens, arról Adatkezelőt kapcsolattartója útján indokolatlan késedelem nélkül, de legfeljebb 24 órán belül értesíti. Adatfeldolgozó indokolatlan késedelem nélkül köteles minden ésszerű lépést megtenni, és minden indokolt intézkedést bevezetni annak érdekében, hogy minimalizálja az adatvédelmi incidensek miatti negatív hatásokat.
Adatfeldolgozó az értesítésében, amennyiben ezen információk a 24 órás határidőn belül rendelkezésre állnak, információt ad 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;
(d) az incidens súlyossága és az elhárítása érdekében tett vagy tervezett intézkedések.

Adatfeldolgozó köteles:
(a) Adatfeldolgozói tevékenysége körében esetlegesen előforduló adatvédelmi incidensekről a mindenkori hatályos jogszabályoknak megfelelő módon és tartalommal belső incidens nyilvántartást vezetni;
(b) Adatkezelő kérésére a belső incidens nyilvántartása másolatának Adatkezelő tekintetében releváns részét rendelkezésre bocsátani; továbbá
(c) Adatkezelő értesítését követően köteles a Nemzeti Adatvédelmi és Információszabadság Hatóság incidens nyilvántartásába az esetlegesen előforduló bejelentés- köteles adatvédelmi incidenseket bejelenteni.