1101/191-1/2026

Kiskunsági Erdészeti és Faipari Zrt.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

I. ÁLTALÁNOS RENDELKEZÉSEK

1) Jelen Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: „Szabályzat") célja, hogy szabályozza a KEFAG Kiskunsági Erdészeti és Faipari Zrt. (továbbiakban: KEFAG Zrt./Társaság/Adatkezelő) személyes adatokat érintő adatkezelési tevékenységét, és biztosítsa az adatalanyok magánszférájának védelmét, érintetti jogait, eleget téve a mindenkor hatályos adatvédelmi tárgyú jogszabályok – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), továbbá az EURÓPAI PARLAMENT ÉS TANÁCS (EU) 2016/679 RENDELETE (továbbiakban: GDPR) – rendelkezéseinek.
2) A Szabályzatot a GDPR, valamint az Infotv. 2. § (2) bekezdése szerint azt kiegészítő előírásokra figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.
3) A Szabályzatban alkalmazott fogalmak tekintetében a GDPR 4. cikke szerinti meghatározások az irányadók.
4) A Szabályzat hatálya kiterjed a Társaságnál foglalkoztatott valamennyi munkavállalóra, valamint munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott (a továbbiakban együtt: foglalkoztatott) személyre.
5) Jelen Szabályzat 2026. augusztus 7. napjától hatályos. A korábbi vonatkozó szabályzat jelen Szabályzat hatálybalépésével egyidejűleg hatályát veszti.

II. ADATKEZELŐ ADATVÉDELMI RENDSZERE

1. SZEMÉLYES ADATOK KEZELÉSÉVEL KAPCSOLATOS FELELŐSSÉG

1) A személyes adatok védelméért, az adatkezelés jogszerűségéért a vezérigazgató felel. Ennek keretében szabályzatok útján meghatározza a személyes adatok védelme és az adatkezelés jogszerűsége szempontjából elvárt, megfelelő technikai és szervezési intézkedéseket és rendelkezik azok folyamatos alkalmazásáról és naprakészen tartásáról.
2) A vezérigazgató gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági rendszer működtetéséről, a működéshez szükséges intézkedések megtételéről.
3) A vezérigazgató kijelöli a Társaság adatvédelmi tisztviselőjét.
4) A vezérigazgató meghozza a Társaság tekintetében az adatkezelésre vonatkozó döntéseket.
5) A szervezeti egység vezetője gondoskodik a szervezeti egységen belül az adatvédelmi követelmények érvényre juttatásáról a Szabályzatban vagy más kötelező erejű adatvédelmi

előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról.

6) A Társaságnál foglalkoztatottak a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat. Betartják az adatkezelésre vonatkozó jogszabályokban, más belső szabályzatokban foglalt előírásokat, tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán és az adatvédelmi incidensek gyanújának felismerése érdekében.

2. ADATVÉDELMI TISZTVISELŐ

1) Az adatvédelmi tisztviselőt a vezérigazgató a GDPR 39. cikkben említett feladatok ellátására való alkalmasság alapján jelöli ki.
2) Az adatvédelmi tisztviselő nevét és elérhetőségét Adatkezelő honlapján közzétett adatkezelési tájékoztatók útján nyilvánosan elérhetővé kell tenni, kijelöléséről a foglalkoztatottakat írásban tájékoztatni kell.
3) Az adatvédelmi tisztviselő feladatai:
   a) tájékoztat, szakmai tanácsot ad, naprakész tájékoztatást nyújt az Adatkezelő, továbbá az adatkezelést végző foglalkoztatottak részére a GDPR és az egyéb kötelező erővel bíró uniós vagy hazai adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
   b) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
   c) ellenőrzi GDPR, az egyéb kötelező erővel bíró uniós vagy hazai adatvédelmi rendelkezések, valamint a Szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását, ennek keretei között az egyes adatkezelési műveletekhez kapcsolódó egyértelmű feladatmeghatározást, az adatkezelési műveletekben közreműködő foglalkoztatottak adatvédelmi ismereteinek bővítését és tudatosságnövelését, valamint a rendszeres időközönként lefolytatandó vizsgálatok megvalósulását;
   d) szakmai tanácsot ad adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését;
   e) közreműködik az adatvédelmi incidens kezelésének folyamatában a GDPR-ban meghatározott módon;
   f) kapcsolattartó pontként szolgál a felügyeleti hatóság felé;
   g) kivizsgálja az érintettek panaszait és kezdeményezi az adatkezelőnél, illetve adatfeldolgozónál a panasz orvoslásához szükséges intézkedések megtételét;
   h) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot.

3. A SZEMÉLYES ADATOK KEZELÉSÉNEK ALAPELVEI

1) A személyes adatok védelme érdekében a KEFAG Zrt. az alábbi adatvédelmi jogi alapelvek mentén szervezi adatvédelmi rendszerét:
   a) Személyes adat kezelésének jogszerűnek, tisztességesnek, az érintett számára átláthatónak kell lennie.
   b) Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
   c) Az adatkezelés céljai szempontjából a személyes adatok megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
   d) Az adatkezelés során biztosítani kell az adatok pontosságát és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét.
   e) Az adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé.
   f) Az adatkezelés során arra alkalmas műszaki vagy szervezési – így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító – intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.
2) A személyes adatok kezelését adatkezelő olyan módon végzi, hogy képes legyen a fenti alapelveknek történő megfelelés igazolására.
3) A személyes adatvédelemmel kapcsolatos szabályozásra és ennek módosítására történő javaslattétel az adatvédelmi tisztviselő feladata. Ha a KEFAG Zrt. bármely foglalkoztatottja személyes adatkezelést érintő körülményt érzékel (így különösen, ha valamely érintett adatkezelést illető kérelme érkezik hozzá, adatvédelmi incidenst tapasztal, vagy bármely egyéb releváns információ birtokába jut), haladéktalanul köteles értesíteni az adatvédelmi tisztviselőt, és továbbítani neki a releváns dokumentumokat.

4. A KÖZÉRDEKŰ ÉS KÖZÉRDEKBŐL NYILVÁNOS ADATOK MEGISMERÉSÉRE IRÁNYULÓ KÉRELMEK TELJESÍTÉSÉNEK RENDJE

1) A közérdekű és közérdekből nyilvános adat megismerése iránt szóban, írásban vagy elektronikus úton bárki igényt nyújthat be.
2) Az adatigénylés részletes szabályait a közérdekű adatok megismerésére irányuló igények teljesítési rendjéről szóló szabályzat rögzíti, amely a www.kefag.hu honlapról elérhető elektronikus formában.

III. A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM

1. ADATKEZELÉS KIALAKÍTÁSÁVAL ÖSSZEFÜGGŐ KÖTELEZETTSÉGEK

1) Adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során megfelelő technikai és szervezési intézkedéseket hajt végre. Mindezek célja az adatvédelmi elvek hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.
2) Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre.
3) A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatályba lépése előtt az SZMSZ alapján a feladat ellátásáért felelős szervezeti egység vezetője kezdeményezi az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát a vezérigazgató felé az adatvédelmi tisztviselő útján.
4) Az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője meghatározza megkeresésében a tervezett adatkezelés legfontosabb jellemzőit:
   a) az adatok kezelésére okot adó körülményt vagy jogszabályi rendelkezést;
   b) a feladat ellátásához szükséges adatköröket és azok tervezett forrását;
   c) a tervezett vagy jogszabályban meghatározott megőrzési időt, vagy az annak meghatározásához szükséges szempontokat;
   d) adattovábbítás címzettjeit;
   e) az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.
5) Az adatvédelmi tisztviselő véleményével együtt továbbítja a megkeresést a vezérigazgató felé, egyidejűleg javaslatot tesz részére
   a) az ahhoz kapcsolódóan szükségesnek tartott további szervezési és technikai intézkedésekre, vagy a GDPR 5. cikkében foglalt alapelveknek megfelelő adatkezelés kialakításának szempontjaira nézve;

b) a kapcsolódó adatvédelmi hatásvizsgálat szükségessége kapcsán;

c) az ahhoz kapcsolódó adatkezelési tájékoztató tartalmára és közzétételére vonatkozóan.

6) Az adatvédelmi tisztviselő javaslata kapcsán a vezérigazgató által hozott döntésről az adatvédelmi tisztviselő tájékoztatja a személyes adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetőjét. A tevékenység adatvédelmi nyilvántartásba történő bejegyzéséről az adatvédelmi tisztviselő gondoskodik.

7) A KEFAG Zrt. 100%-os állami tulajdonban lévő gazdálkodó szervezet, ezért adatkezelési tevékenységeit elsődlegesen a GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalapra alapíthatja.

8) Egyéb a GDPR 6. cikkében foglalt jogalap abban az esetben hivatkozható az adatkezelés jogalapjaként, ha az adatkezelési tevékenység nem szükséges a Adatkezelő közfeladatának ellátásához.

9) Az előző pontban foglaltakon túl akkor képezheti Adatkezelő adatkezelésének jogalapját a GDPR 6. cikk (1) bekezdés a) pontja szerinti érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és Adatkezelő között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.

2. AZ ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA

1) A Társaság az adatkezelési tevékenységeinek nyilvántartását az adatvédelmi tisztviselő vezeti.

2) Az adatkezelési tevékenységek nyilvántartása a GDPR 30. cikke által meghatározott módon történik, amelynek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatókban foglaltakkal.

3. ADATVÉDELMI HATÁSVIZSGÁLAT ÉS ELŐZETES KONZULTÁCIÓ

1) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az Adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

2) Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az Adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal.
3) Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.
4) Adatvédelmi hatásvizsgálatot a GDPR 35. cikke értelmében különösen az alábbi esetekben kell elvégezni:
   a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen - ideértve a profilalkotást is -alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
   b) a GDPR 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
   c) nyilvános helyek nagymértékű, módszeres megfigyelése.
5) Adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni, ezt követően elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait.
6) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoportba a tervezett adatkezeléssel érintett szervezeti egységek kötelesek résztvevőt kijelölni.
7) Az adatvédelmi hatásvizsgálatra vonatkozó hatályos uniós és hazai iránymutatásokban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni.
8) A munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól jelentést készít a vezérigazgatónak.
9) Az adatvédelmi hatásvizsgálatot lefolytató munkacsoport munkáját az adatvédelmi tisztviselő – és amennyiben az adatkezelés elektronikus információs rendszert is érint, az elektronikus információs rendszer biztonságáért felelős személy – segíti.
10) Az adatvédelmi hatásvizsgálatról készült jelentést és a kapcsolódó véleményeket a vezérigazgató részére írásban kell előterjeszteni. A tervezett adatkezelés nem kezdhető meg, amíg a vezérigazgató el nem fogadja az adatvédelmi hatásvizsgálat eredményes lezárultáról, és az abban a kockázatok csökkentését szolgáló intézkedések bevezetéséről és az adatkezelés

jóváhagyásáról szóló jelentést, vagy az adatvédelmi hatásvizsgálat mellőzésének, vagy megszüntetésének okait tartalmazó jelentést.

4. ADATKEZELÉSI TÁJÉKOZTATÁS

1) Adatkezelő adatkezelési tevékenységeire vonatkozóan a GDPR 13-14. cikke szerinti tartalommal szükséges az adatkezelési tájékoztatókat összeállítani.
2) Az adatkezelési tájékoztatókban foglaltak naprakészségét és elérhetőségét az adatvédelmi tisztviselő és az SZMSZ-ben meghatározott feladataihoz kötődően a tevékenység ellátásáért felelős szervezeti egység is köteles figyelemmel kísérni.
3) A kizárólag Adatkezelő foglalkoztatottjait érintő adatkezelési célok kapcsán összeállított adatkezelési tájékoztatókat zárt informatikai rendszerben kell a foglalkoztatottak számára elérhetővé tenni.
4) A foglalkoztatotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, elektronikus úton szükséges megküldeni az őket érintő adatkezelési tájékoztatókat.
5) Adatkezelőnél személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről a papíralapú adatkezelési tájékoztató, valamint figyelemfelhívó jelzés útján kell tájékoztatni.
6) További érintetti kör esetében Adatkezelő honlapján, az „Adatkezelési tájékoztatók" cím alatt közzétéve bocsátja az érintettek rendelkezésére a szükséges tájékoztatást.

5. ADATBIZTONSÁGI KÖVETELMÉNYEK

1) Adatkezelő a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető kockázatok mértékéhez igazodó technikai és szervezési intézkedéseket foganatosít, amely során figyelembe veszi az adatkezelés összes körülményét, így különösen:
   a) tudomány és technológia mindenkori állását,
   b) a megvalósítás költségeit,
   c) adatkezelés jellegét, hatókörét, körülményeit és céljait,
   d) az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.
2) A Társaság papíralapon, ill. számítógépes hálózaton végzi a személyes adatok tárolását. A papíralapú adattárolás megfelelően zárható helyiségben történik oly módon, hogy az illetéktelen személy által ne legyen hozzáférhető vagy megismerhető.

a) Zárt szerverszobában lévő szerverek alkalmazása, a szerverszoba fizikai védelemmel ellátott klimatizált helyiségben van.
b) A cég hálózata az Internet irányába zárt, tűzfallal védett, hálózaton kívüli eszközök csak egyedi megoldásokkal (VPN) tudnak csatlakozni a belső hálózathoz.
c) Adatok mentése esténként saját külső telephelyünkön lévő fizikailag zárt helyiségben található szerverre.
d) Időszakonként meghajtó titkosítással védett külső tároló eszközre.
e) Zárható irodában található asztali számítógépen, meghajtó titkosítással védett külső eszközökön, laptopokon. Szerverszobában található fájlszerver, jelszóval védett megosztásában.

3) A KEFAG Zrt. adatbiztonsági intézkedéseivel biztosítja
a) az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását,
b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását,
c) azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
d) azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön.

IV. AZ ADATVÉDELMI INCIDENSEK KEZELÉSE

1) Az adatvédelmi incidenst adatkezelő haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő 72 órán belül bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. A bejelentést a hatóság által megadott formában és módon kell megtenni, a hatóság előírásai szerint a hatóság által megjelölt elektronikus felületen. Ha adatkezelő a bejelentési kötelezettséget akadályoztatása miatt határidőben nem teljesíti, azt az akadály megszűnését követően haladéktalanul teljesíti, és a bejelentéshez mellékeli a késedelem okait feltáró nyilatkozatát is.
2) A munkavállaló köteles jelenteni a szervezeti egység vezetőjének, ha adatvédelmi incidens, vagy arra utaló információk jutottak a tudomására.
3) A szervezeti egység vezetője vagy az általa kijelölt személy a jelzést követően azonnal tájékozódik az eset lényeges körülményeiről. Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, soron kívül

megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.

4) Az IV.3. pont szerinti értesítés az adatvédelmi incidens bekövetkeztének, illetőleg az általa az érintettre nézve jelentett kockázatok és annak hatásainak megállapítása érdekében tartalmazza legalább
   a) az adatvédelmi incidens jellegét és rövid leírását, ideértve különösen az észlelés és bekövetkezés feltételezett időpontját, az érintett rendszer vagy irat megjelölését;
   b) a valószínűsíthetően érintett személyek körét;
   c) a valószínűsíthetően érintett személyes adatok kategóriáit, nagyságrendjét;
   d) az általa megtett halaszthatatlan intézkedéseket;
   e) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságát, az általa tervezett további intézkedések leírását.
5) Az adatvédelmi tisztviselő megvizsgálja az értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja a Hatóság informatikai biztonságért felelős vezetőjét, a szervezeti egység vezetőjét vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.
6) Abban az esetben, ha az adatvédelmi incidens feltételezhetően a Társaság által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő a Társaság informatikai biztonságért felelős vezetője felé is köteles jelezni a bejelentést. A Társaság informatikai biztonságért felelős vezetője a jelzést követően köteles haladéktalanul véleményt összeállítani az adatvédelmi tisztviselő részére arról, hogy az adatvédelmi incidens valóban érinti-e az informatikai rendszer biztonságát, és ismerteti az ezzel kapcsolatos javasolt, valamint megtett intézkedéseket.
7) Amennyiben az adatvédelmi incidens a Társaság által igénybevett adatfeldolgozó tevékenységével kapcsolatban következett be, az adatvédelmi incidens körülményeinek, és az azzal összefüggő lehetséges kockázatok és hatások kivizsgálásába az adatfeldolgozó képviselőjét is be kell vonni.
8) Az adatvédelmi tisztviselő vizsgálata keretében mérlegeli az adatvédelmi incidens következtében az érintettekre nézve megjelenő kockázatokat. Ennek során legalább a következőket veszi figyelembe:
   a) az adatvédelmi incidens jellegét;
   b) az érintettek körét, hozzávetőleges számukat;
   c) az incidenssel érintett adatok kategóriáit, az érintett különleges adatokat és a GDPR preambulumának (75) bekezdése szerinti szenzitív adatokat és azok hozzávetőleges számát, illetve nagyságrendjét;
   d) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

e) minden, az adatvédelmi incidens megoldására tett vagy tervezett intézkedést, ideértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

f) az elektronikus információbiztonságot is érintő incidensek esetén az elektronikus információbiztonságért felelős vezető által azonosított további kockázatot;

g) az adatvédelmi incidensek kezelése és a kapcsolódó kockázatok mérlegelése tárgyában az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott – iránymutatást;

h) az adatkezelés kapcsán korábban lefolytatott adatvédelmi hatásvizsgálat dokumentációját.

9) Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja a vezérigazgatót az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószínűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.

10) A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.

11) Amennyiben a vezérigazgató a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő a NAIH honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a Hatóság által vezetett nyilvántartásba.

12) Az adatkezelő – az adatvédelmi tisztviselő útján – az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése céljából nyilvántartást vezet, amely tartalmazza az adatvédelmi incidensről készült feljegyzés iktatószámát, az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs rendszer megjelölését vagy azonosítóját, az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját, az érintett személyes adatok körét, az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket, a 25. § (3) és (4) bekezdés szerinti bejelentés időpontját – amennyiben az adatvédelmi incidenst a Hatóság részére a GDPR 33. cikk (1) bekezdése szerint bejelentették, vagy annak rövid indokolását, ami miatt az adatvédelmi incidenst nem jelentették be..

V. AZ ÉRINTETTI JOGGYAKORLÁS BIZTOSÍTÁSA

1) Adatkezelő bármely adatkezelésére vonatkozó érintetti joggyakorlásra irányuló megkeresés kapcsán vizsgálja azt, hogy a kérelmet benyújtó természetes személy személyazonossága

megállapítható -e. A kérelmet benyújtó természetes személy azonosítása érdekében kizárólag az adott célra szükséges és elégséges többlet személyes adat kérhető.

2) Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni.

3) Az érintetti joggyakorlásra utaló beadványok kapcsán – az adatvédelmi tisztviselő bevonásával – mindenekelőtt meg kell állapítani, hogy abban az általános adatvédelmi rendelet szerinti valamely érintetti jogot, különösen a GDPR 15. cikke szerinti hozzáférési jogot, vagy közérdekű adatigénylést kíván-e előterjeszteni.

4) Adatkezelő indokolatlan késedelem nélkül és a lehető legrövidebb időn belül, de legkésőbb az azonosítható érintettől származó kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről.

5) Amennyiben annak a GDPR 12. cikkében foglalt feltételei fennállnak, a válaszadás határideje további két hónappal meghosszabbítható, azonban ennek megítélése kapcsán részére határidőn belül, írásban kell igazolni a késedelem okait.

6) Az érintett jogorvoslatért a NAIH-hoz (név: Nemzeti Adatvédelmi és Információszabadság Hatóság, székhely: 1055 Budapest, Falk Miksa utca 9-11., levelezési cím: 1363 Budapest, Pf. 9.; telefon: +36-1-391-1400, e-mail: ugyfelszolgalat@naih.hu) vagy a bírósághoz (http://birosag.hu) fordulhat.

Kecskemét, 2026. augusztus 7.

Sulyok Ferenc
vezérigazgató

KEFAG Kiskunsági Erdészeti
és Faipari Zrt.