**24/2022. sz.**
**vezérigazgatói utasítás**

**az Adatkezelési és Adatvédelmi Szabályzatról**

A Diákhitel Központ Zrt. Igazgatóságának 20/2021. (V. 27.) sz. Ig. határozatával elfogadott, a Diákhitel Központ Zrt. Szervezeti és Működési Szabályzatáról szóló 31/2021. sz. vezérigazgatói utasítás mellékletének 14. § (8) bekezdés c) pontjában foglalt felhatalmazás alapján az alábbiakat rendelem el:

**1. §** Jelen utasítás mellékleteként kiadom és alkalmazni rendelem a Diákhitel Központ Zrt. Adatkezelési és Adatvédelmi Szabályzatát.

**2. §** (1) Jelen utasítás az aláírásának napján lép hatályba, rendelkezéseit a hatálybalépés napjától kell alkalmazni.

(2) Jelen utasítás hatályba lépésével egyidejűleg hatályát veszti a Diákhitel Központ Zrt. Adatkezelési és Adatvédelmi Szabályzatáról szóló 18/2021. sz. vezérigazgatói utasítás.

Budapest, 2022. május 18.

DK0000242280

Havelda Balázs
pénzügyi vezérigazgató-
helyettes

# A DIÁKHITEL KÖZPONT ZRT.

# ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZAT

# I. FEJEZET
# ÁLTALÁNOS RENDELKEZÉSEK

## A szabályozás célja, alapja

**1. §** (1) Az Adatkezelési és Adatvédelmi Szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a Diákhitel Központ Zrt. (a továbbiakban: DHK Zrt.) személyes adatkezeléseinek törvényes rendjét, és ezzel biztosítsa az általa nyilvántartott személyes adatok védelmét.

(2) A Szabályzat megalkotásának alapja az Európai Unió Általános Adatvédelmi Rendeletének - az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló rendelet - (a továbbiakban: GDPR) (78) preambulumbekezdésében és 24. cikk (2) bekezdésében foglalt, az adatkezelési tevékenység vonatkozásában a beépített és alapértelmezett adatvédelem elvét biztosító intézkedéseket meghatározó arányos, megfelelő adatvédelmi szabályok alkalmazásából eredő szabályozási kötelezettség.

## A Szabályzat hatálya

**2. §** (1) A Szabályzat tárgyi hatálya kiterjed a DHK Zrt. működésével összefüggő valamennyi személyes adatkezelésére függetlenül az adatkezelés céljától és módszerétől.

(2) A Szabályzat személyi hatálya kiterjed a DHK Zrt. valamennyi munkavállalójára.

(3) A Szabályzat rendelkezéseit a hatálybalépés időpontját megelőzően nyilvántartásba vett vagy keletkezett, már kezelt adatok tekintetében is alkalmazni kell

## Alkalmazandó jogszabályok és belső szabályzatok

**4. §** (1) Jelen Szabályzatot az alábbi jogszabályok – illetőleg az esetlegesen később ezek helyébe lépő jogszabályok – rendelkezéseinek figyelembevételével, azok rendelkezéseivel összhangban, velük együttesen kell alkalmazni:

a) az Európai Parlament és a Tanács 2016/679. számú Általános Adatvédelmi Rendelete (GDPR)
b) Magyarország Alaptörvénye;
c) a Polgári Törvénykönyvről szóló 2013. évi V. törvény;
d) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.);
e) a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény;
f) az oktatási nyilvántartásról szóló 2018. évi LXXXIX. törvény;
g) a Munka Törvénykönyvéről szóló 2012. évi I. törvény;
h) az adózás rendjéről szóló 2017. évi CL. törvény;

i) a számvitelről szóló 2000. évi C. törvény,
j) a központi hitelinformációs rendszerről szóló 2011. évi CXXII. törvény;
k) a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény;
l) a hallgatói hitelrendszerről és a Diákhitel Központról szóló 1/2012. (I. 20.) Kormányrendelet;
m) a felnőttképzésről szóló 2013. évi LXXVII. törvény;
n) a szakképzésről szóló 2019. évi LXXX. törvény;
o) a köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény;
p) a közbeszerzésekről szóló 2015. évi CXLIII. törvény.

(2) Az egyes adatvédelmi tárgyú fogalmak tekintetében a GDPR szerinti meghatározások irányadók.

**5. §** (1) A DHK Zrt-hez beérkező, illetve a DHK Zrt-nél keletkeztetett iratok készítésének, kezelésének, nyilvántartásának és selejtezésének szabályait az Iratkezelési Szabályzattal összhangban kell alkalmazni.

(2) A DHK Zrt. elektronikus rendszereiben kezelt személyes adatok védelmére vonatkozóan jelen szabályzatot az Információbiztonsági Szabályzat rendelkezéseivel összhangban kell alkalmazni.

## II. FEJEZET
## ADATKEZELÉSSEL ÖSSZEFÜGGŐ FELELŐSSÉGI KÖRÖK

### A vezérigazgató felelősségébe tartozó feladatkörök

**6. §** (1) A DHK Zrt. által kezelt személyes adatok védelméért és az adatkezelés jogszerűségéért a vezérigazgató felel.

(2) A vezérigazgató az (1) bek. szerinti felelősségi körében a következő feladatokat látja el:

a) a Normaalkotási Szabályzatban foglaltaknak megfelelően vezérigazgatói utasítással kiadott szabályzatokban rendelkezik azon technikai és szervezési intézkedésekről, amelyek a személyes adatok védelmének jogszerűségét biztosítják;
b) meghozza a személyes adatok kezelésére vonatkozó döntéseket;
c) gondoskodik a közérdekű, illetve közérdekből nyilvános adatok Infotv. szerinti kötelező közzétételéről, valamint a közérdekű adatigénylések teljesítéséről;
d) kijelöli a DHK Zrt. adatvédelmi tisztviselőjét;
e) gondoskodik az adatvédelemhez szükséges erőforrások biztosításáról.

### Az igazgatók felelősségi körébe tartozó feladatok

**7. §** A Szervezeti és Működési Szabályzatban meghatározott, irányításuk alatt álló szervezeti egység tekintetében:

a) a személyes adatok védelmét biztosító technikai és szervezési intézkedésekről – amennyiben a 6. § (2) bek. a) pont szerinti szabályzatokhoz képest speciális rendelkezések szükségesek - ügyviteli utasítást adnak ki a Normaalkotási Szabályzatnak megfelelően;
b) gondoskodnak a szakterületük tevékenységét érintő adatvédelmi követelmények érvényre juttatásáról, ennek körében szükség esetén ellenőrzést rendelnek el;
c) kijelölik a személyes adatok kezelésére jogosult munkavállalókat és meghatározzák adatkezelési, hozzáférési jogosultságaikat;
d) a szakterületük feladatkörébe tartozó, nem informatikai rendszer adatbiztonsági követelményeknek való meg nem felelésére (hanem pl. ügyintézői hibára vagy mulasztásra) visszavezethető adatkezelési tevékenység során bekövetkező adatvédelmi incidenseket az adatvédelmi tisztviselő és szükség esetén az információbiztonsági felelős bevonásával, amelynek során sor kerül az incidens körülményeinek feltárására, a bekövetkezett incidens pontos meghatározására, az érintettek és az érintett személyes adatok meghatározására, valamint az incidenst okozó körülmény azonnali elhárítására, továbbá hasonló incidens későbbi felmerülését lehetővé tevő körülmények elhárítását célzó intézkedések előkészítésére.

### A DHK Zrt. munkavállalói felelősségi körébe tartozó feladatok

**8. §** (1) Valamennyi munkavállaló köteles a 6-7. § szerinti belső szabályzatokban, ügyviteli utasításokban foglalt, adatvédelemmel összefüggő, a munkakörét érintő

rendelkezést megismerni és betartani. Amennyiben valamely belső szabályzat esetleges hibáját, hiányosságát tapasztalják, kötelesek jelezni közvetlen vezetőjük felé. Amennyiben valamely adatkezelési művelet (pl. személyes adat felvétele, módosítása, átadása vagy törlése) vonatkozásában kétségük merül fel – akár tartalmaz rá belső szabályzat rendelkezést, akár nem – a művelet végrehajtását megelőzően kötelesek egyeztetést kezdeményezni az adatvédelmi tisztviselővel.

(2) A munkavállalók kizárólag a hozzáférési jogosultságaik keretein belüli feladatokat jogosultak ellátni. Amennyiben a munkaköri feladatuk ellátásához a részükre meghatározott jogosultsági kör hatóköre nem elegendő, haladéktalanul kötelesek ezt jelezni közvetlen vezetőjük felé.

(3) A munkavállalók kötelesek az informatikai rendszerek kezeléséhez szükséges jelszavak bizalmasságát kiemelt gondossággal biztosítani – belépéshez vagy adatkezelési művelethez szükséges jelszó nem adható át senkinek.

(4) Az ügyféladatokat kezelő munkavállalók kiemelt figyelemmel kezelik az érintetti jogok gyakorlása iránti kérelmeket (tájékoztatás, hozzáférés, helyesbítés, törlés, korlátozás, adathordozás, tiltakozás). Amennyiben ilyen kérelem érkezik – figyelemmel az egy hónapos ügyintézési határidőre – haladéktalanul egyeztetést kezdeményeznek a közvetlen vezetőjük útján az adatvédelmi tisztviselővel.

(5) A munkavállalók kötelesek a munkájuk során esetlegesen észlelt adatvédelmi incidenst vagy incidens gyanúját haladéktalanul jelenteni a közvetlen vezetőjük és az adatvédelmi tisztviselő felé, és az incidens kivizsgálása során aktívan közreműködni.

## Az adatvédelmi tisztviselő felelősségi körébe tartozó feladatok

**9. §** (1) Az adatvédelmi tisztviselő a következő feladatokat látja el:

a) vezeti a DHK Zrt. adatvédelmi nyilvántartását, és azt közzéteszi a valamennyi munkavállaló számára elérhető belső portál „Adatvédelem" c. aloldalán;
b) adatvédelmi szempontból véleményezi az általános szerződési feltételeket tartalmazó Üzletszabályzatok mellékletét képező Adatkezelési Tájékoztatókat;
c) adatvédelmi szempontból véleményezi a DHK Zrt. adatfeldolgozási tárgyú szerződéseit, és gondoskodik a kötelező szerződéses tartalmak beépítéséről;
d) közreműködik a DHK Zrt. adatkezelését érintő jogszabály-tervezetek előkészítésében, az elkészült tervezeteket erre irányuló felkérés esetén véleményezi;
e) megvizsgálja a DHK Zrt. új vagy módosuló adatkezeléseinek érintettre gyakorolt kockázatát, hatását, szükség esetén közreműködik az adatvédelmi hatásvizsgálatot lefolytatásában;
f) kezdeményezi és lefolytatja a DHK Zrt. munkatársainak adatvédelmet tudatosító képzéseit, oktatásait, továbbá szükség esetén adatvédelmi ellenőrzést folytat le;
g) évente felülvizsgálja az Adatvédelmi Szabályzat gyakorlati érvényesülését,
h) elősegíti az érintetteket megillető jogok gyakorlását, véleményezi az érintetti kérelmek, kifogások alapján tervezett intézkedéseket, illetve az ezekről szóló válaszlevél-tervezeteket;

i) erre irányuló kérdés esetén adatvédelmi állásfoglalást ad a szervezeti egységek vezetői részére;
j) adatvédelmi incidens esetén kontrollálja annak kivizsgálását, kockázatértékelését, véleményezi a szükség esetén eszközölt intézkedések tervezetét, felkérés esetén állást foglal a Nemzeti Adatvédelmi és Információszabadság Hatóság felé történő bejelentés szükségességéről, illetve az érintettek tájékoztatásáról, továbbá közreműködik a hasonló incidens jövőben történő elkerülését biztosító intézkedések kidolgozásában;
k) a vezérigazgató bevonásával kapcsolatot tart a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

(2) Az adatvédelmi tisztviselő jogosult:
a) az (1) bek. szerinti feladatai ellátása során bármely munkavállalótól vagy vezetőtől tájékoztatást, felvilágosítást kérni adatkezelést érintő kérdésben;
b) részt venni a DHK Zrt. személyes adatkezelését érintő bármely egyeztetésen és ott véleményt megfogalmazni vagy javaslatot tenni;
c) az adatkezelési tevékenységeket szabályozó rendelkezések vonatkozásában belső szabályzat módosítását javasolni, vagy új szabályzat kiadását kezdeményezni.

## Információbiztonsági felelős feladatai

**10. §** (1) Az információbiztonsági felelős – külső szakértő esetén erre irányuló megbízás alapján – köteles az információs rendszerek működését meghatározó követelmények kialakítása során érvényesíteni az adatbiztonsági elvárásokat annak érdekében, hogy a DHK Zrt. által kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított legyen. Ennek körében közreműködik az új informatikai rendszerek bevezetését vagy már működő rendszerek módosítását megelőzően IT biztonsági kockázatelemzést – szükség esetén sérülékenységi vizsgálatot lefolytatni – lefolytatni, illetve erre az informatikai igazgatónál javaslatot tenni.

(2) Az információbiztonsági felelős folytatja le a DHK Zrt. informatikai rendszereit érintő adatvédelmi incidenseket az adatvédelmi tisztviselő, az IT üzemeltetési osztályvezető és az incidenssel érintett adatkezelési folyamat szerint illetékes szervezeti egység vezetőjének bevonásával az incidens körülményeinek feltárásában, a bekövetkezett incidens pontos meghatározásában, az érintettek és az érintett személyes adatok meghatározásában, valamint az incidenst okozó körülmény azonnali elhárításában, továbbá hasonló incidens későbbi felmerülését lehetővé tevő körülmények elhárítását célzó intézkedések előkészítésében.

## III. FEJEZET
## A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATKEZELÉS ELVÉNEK ÉRVÉNYESÜLÉSE

### Új adatkezelés megkezdéséhez szükséges követelmények

**11. §** (1) Amennyiben a DHK Zrt. valamely szakterülete személyes adatkezeléssel járó új üzleti folyamatot tervez bevezetni, ezen szakterület vezetője már a döntéshozatal előkészítésébe köteles bevonni az adatvédelmi tisztviselőt.

(2) Az adatvédelmi tisztviselő a tervezett adatkezeléssel összefüggésben annak célja, módja, az adatkezelést támogató nyilvántartási vagy informatikai rendszer felépítése, az adatkezelési folyamatokban részt vevő munkatársak feladat és hatásköre vonatkozásában jogosult információt kérni, és javaslatot tenni a tervezett folyamat esetleges módosítására.

(3) Amennyiben az új adatkezelés új informatikai rendszer bevezetését is igényli, az adatvédelmi tisztviselő javaslatára az információbiztonsági felelőst is be kell vonni a döntéselőkészítésbe.

**12. §** (1) Új adatkezelés csak abban az esetben vezethető be, ha az megfelel a GDPR alapelveinek, az érintetti jogok korlátozás nélkül biztosíthatók, az adatkezelő rendszer megfelel az adatbiztonság követelményeinek, és az adatkezeléssel összefüggő feladat- és hatáskörök egyértelműen rögzítésre kerülnek.

(2) Amennyiben az adatvédelmi tisztviselő úgy ítéli meg, hogy adatvédelmi hatásvizsgálat lefolytatására van szükség, az új folyamat bevezetésére addig nem kerülhet sor, amíg az adatvédelmi hatásvizsgálatot az érintett szakterület vezetője – az információbiztonsági felelős és az adatvédelmi tisztviselő bevonásával – le nem folytatta, és a hatásvizsgálat eredményeként vezetői döntés nem született arról, hogy az adatkezelés nem jár olyan, a DHK Zrt. által nem kezelhető kockázattal, amely a Nemzeti Adatvédelmi és Információszabadság Hatóság döntését igényli. A hatósággal lefolytatandó előzetes konzultációt az adatvédelmi tisztviselő kezdeményezi és koordinálja.

(3) Az új adatkezelés folyamatának kialakítása során az adatvédelmi tisztviselő véleményezi az üzleti folyamat, illetve az azt támogató informatikai rendszer követelményjegyzékét adatvédelmi szempontból. Az adatvédelmi tisztviselő véleményét az új folyamatot bevezetni tervező szakterület vezetője köteles megfelelően figyelembe venni, és szükség esetén együttműködés útján ezen dokumentumokat módosítani.

**13. §** Az új adatkezelési tevékenység – az adatbiztonság követelményének megfelelő műszaki feltételek ellenőrzésén és sikeres tesztelésén - csak akkor indulhat el, ha az adatvédelmi tisztviselő előzetes véleményezése és javaslatai alaján:

a) előkészítésre és véglegesítésre került az érintettek előzetes tájékoztatását szolgáló dokumentum,
b) az esetlegesen igénybe vett adatfeldolgozókkal aláírásra került az adatfeldolgozási tevékenység ellátására kötött szerződés;

c) adattovábbítással járó adatkezelés esetén az adattovábbítás jogszerűségének feltételei ellenőrzésre kerültek, szükség esetén erről a címzettel szerződés vagy együttműködési megállapodás köttetett.

## Folyamatban lévő adatkezelés módosításához szükséges követelmények

**14. §** Amennyiben a DHK Zrt. valamely szakterülete egy már korábban bevezetett adatkezelési folyamatot módosítani kíván – így pl. új személyes adat-kategóriákat von be az adatkezelésbe, annak célját vagy időtartamát módosítja vagy az adatkezelés módszerét jelentősen megváltoztatja – a 11-13. §-ban foglalt követelmények és feltételek megfelelően irányadók ezen döntés meghozatalára, illetőleg a módosuló adatkezelési tevékenység megkezdésére.

## Az adatbiztonsági követelmények

**15. §** (1) A DHK Zrt. a személyes adatok kezelése során azok bizalmasságát, sértetlenségét és rendelkezésre állását biztosító, az érintettekre nézve megjelenő kockázatokkal arányos zárt, teljes körű és folyamatos szervezési és technikai védelmi intézkedéseket alkalmaz. Az informatikai rendszerekben kezelt adatok biztonságára vonatkozóan – ezen belül különösen a hozzáférési jogosultságokról, a mentésekről, az üzletmenet folytonosságáról és az esetleges katasztrófahelyzeteket követő visszaállításról - a DHK Zrt. Információbiztonsági Szabályzata rendelkezik.

(2) Az (1) bek. szerinti védelmi intézkedések naprakészen tartása érdekében bármely szervezeti egység vezetője, illetőleg az adatvédelmi tisztviselő és az információbiztonsági felelős jogosult a vezérigazgatónak javaslatot tenni azok pontosítására vagy továbbfejlesztésére.

**16. §** (1) A DHK Zrt. személyes adatokat tartalmazó nyilvántartásaihoz, illetve személyes adatokat kezelő informatikai rendszereihez a munkavállalók csak megfelelően kialakított jogosultsági rendszer alkalmazásával férhetnek hozzá. A jogosultsági rendszer alapja az, hogy az adott munkavállaló munkakörének ellátásához nélkülözhetetlen-e a személyes adatok megismerése.

(2) A jogosultsági rendszer alkalmazásával való hozzáférési jog biztosítására vagy visszavonására az érintett munkavállaló szervezeti egységének vezetője jogosult. A jogosultságokat a DHK Zrt. valamennyi szervezeti egység vezetőjének bevonásával évente felülvizsgálja.

**17. §** (1) Személyes adatokat tartalmazó dokumentumok, nyilvántartások kizárólag a DHK Zrt. által a munkavállalók rendelkezésére bocsátott számítástechnikai eszközökön tárolhatók. Ezen eszközök kockázatokkal arányos védelméről – így a jogosulatlan hozzáférést megakadályozó tűzfalbeállítások alkalmazásáról és a vírusvédelmi rendszerek folyamatos működtetéséről - az informatikai üzemeltetési terület gondoskodik.

(2) Személyes adatokat tartalmazó papíralapú dokumentumok vagy ilyen adatokat tartalmazó optikai/elektronikus adathordozók csak az érintett munkavállaló szervezeti egysége vezetőjének engedélyével vihetők ki a DHK Zrt. székhelyéről.

**18. §** (1) Amennyiben a DHK Zrt. adatfeldolgozónak nem minősülő külső partnert vesz igénybe olyan feladat ellátására, amelyhez személyes adatok átadása vagy rendelkezésre bocsátása nélkülözhetetlen, arra – amennyiben a címzett nem tartozik a hivatása szerinti, jogszabályban meghatározott titoktartási kötelezettség alá (pl. ügyvéd, foglalkozásegészségügyi vizsgálatot végző szakorvos) - kizárólag titoktartási nyilatkozat aláírását követően kerülhet sor.

(2) Adatfeldolgozó részére személyes adat kizárólag olyan írásbeli adatfeldolgozási szerződés alapján adható át vagy bocsátható rendelkezésre, amely megfelel a GDPR 28. cikkében meghatározott kötelező tartalmi elemeknek. A szerződés tartalmi megfelelését a szerződés aláírását megelőzően az adatvédelmi tisztviselő vizsgálja.

(3) A DHK Zrt. legértékesebb adatai a hallgatói és képzési hitelszerződét kötő ügyfelek szerződéssel összefüggésben kezelt személyes adatai. Ezen adatok a bizalmasságuk kiemelt fontosságára tekintettel ügyféladatokat kezelő informatikai rendszer tesztelése céljából csak álnevesített formában adhatók át, és csak olyan körben, amely az adott – előre meghatározott hatókörű - teszt eredményes lefolytatása céljából nélkülözhetetlen. Követelmény, hogy a teszt eredményes lefolytatását követően a tesztet lefolytató partner köteles az átadott adatokat a saját rendszereiből törölni.

**19. §** Amennyiben valamely személyes adat kezelésének célja megszűnik, vagy annak törlése más, GDPR 17. cikkében meghatározott okból válik szükségessé, a DHK Zrt. gondoskodik ezen adatok valamennyi nyilvántartásból történő törléséről, vagy ezen adatokat az elektronikus nyilvántartásaiban anonimizálja.

## Az adatkezelés átláthatósága

**20. §** (1) A DHK Zrt. az egyes adatkezelései érintettjeit világos, könnyen értelmezhető és átlátható módon tájékoztatja a GDPR 13-14. cikkeiben foglaltaknak megfelelő tartalommal.

(2) Az (1) bek. szerinti tájékoztatás módja:

a) a munkavállalók a belépésükkel egyidejűleg hozzáférést kapnak az intranetes felület „Adatvédelem" menüpontjához, amely tartalmazza a munkavállalói személyes adatok kezelésével összefüggő részletes tájékoztatót, amely tájékoztatóban foglaltakat a munkaszerződés aláírásával tudomásul vesznek, ezt követően pedig az esetleges változásokról ugyanezen felületen közölt tájékoztató útján értesülnek;

b) a DHK Zrt. ügyfelei a Diákhitel Direkt hiteligénylési felületen, emellett a www.diakhitel.hu hivatalos weboldalon szerződéstípusonként közzétett adatkezelési tájékoztatók útján értesülnek a szerződéssel összefüggésben történő adatkezelésekről;

c) a személyes ügyfélszolgálaton megjelenő ügyfelek és érdeklődők az ügyfélszolgálati helyiség hirdetőtábláján kifüggesztett adatkezelési tájékoztatóból értesülnek személyes adataik kezeléséről;

d) a közérdekű adatigénylést benyújtó kérelmezők a www.diakhitel.hu weboldal Közérdekű Adatok menüpontjában közzétett tájékoztató útján értesülhetnek az adatigényléssel összefüggő személyes adatkezelésről;
e) a DHK Zrt. üzleti partnereinek kapcsolattartói az adott partnerrel kötött szerződésbe foglalt Adatvédelmi Rendelkezések fejezetben értesülhetnek a kapcsolattartással összefüggő adatkezelésről.

## IV. FEJEZET
## ADATVÉDELMI INCIDENSEK KEZELÉSE

**21. §** (1) Amennyiben valamely munkavállaló érintetti bejelentés vagy egyéb megalapozott információ alapján a DHK Zrt. által kezelt személyes adatok vonatkozásában adatvédelmi incidens bekövetkezéséről szerez tudomást, haladéktalanul köteles erről tájékoztatni a közvetlen vezetőjét és az adatvédelmi tisztviselőt.

(2) A szervezeti egység vezetője az adatvédelmi tisztviselővel és informatikai rendszert érintő incidens esetében az információbiztonsági felelőssel történő konzultációt követően haladéktalanul gondoskodik az incidens érintettekre nézve megjelenő hátrányos hatásainak megszüntetéséről vagy csökkentéséről, ennek körében szükség esetén az érintett adatkezelési tevékenységet felfüggeszti.

**22. §** (1) Amennyiben az adatvédelmi incidens nem valamely informatikai rendszer biztonságával, illetve annak hiányosságával kapcsolatban következett be, hanem ügyintézői hiba – pl. jogosulatlan adatfelvétel, adatmódosítás, adattörlés, adatátadás – eredményeként, annak kivizsgálásáról az incidenssel érintett szakterületet vezető igazgató gondoskodik. Amennyiben az adatvédelmi incidens valamely informatikai rendszer biztonságával, illetve annak hiányosságával kapcsolatban – pl. hibás rendszerbeállítás vagy jogosulatlan művelet miatti adatszivárgás - következett be, az incidenst az információbiztonsági felelős vizsgálja ki.

(2) Az adatvédelmi incidens kivizsgálása során az adatvédelmi tisztviselő bevonása minden esetben kötelező, egyéb szakterület vezetője vagy a DHK Zrt. bármely munkavállalója pedig amennyiben szükséges, bevonható.

(3) Az incidens kivizsgálásáról az azt lefolytató legalább a következő tartalmi elemekre kiterjedő jegyzőkönyvet készít:

a) az adatvédelmi incidens jellegét és rövid leírását, az észlelés körülményeit, a bekövetkezés feltételezett időpontját és okát, valamint az érintett üzleti folyamat, informatikai rendszer vagy irat megjelölését;

b) a valószínűsíthetően érintett személyek körét és számát;

c) az általa megtett 21. § (2) bek. szerinti intézkedéseket;

d) az érintettekre gyakorolt hatást;

e) azon intézkedéseket, amelyek a hasonló incidensek elkerülése érdekében nélkülözhetetlenek.

(4) A kivizsgálást úgy kell lefolytatni, hogy annak szükség esetén kötelező bejelentésére az incidens észlelését követő 72 órán belül sor kerülhessen.

(5) Az adatvédelmi incidensek nyilvántartását az adatvédelmi tisztviselő végzi a lefolytatott vizsgálat eredményei alapján. A nyilvántartás a következőket tartalmazza:

a) adatvédelmi incidenshez kapcsolódó tények, körülmények (különösen: mikor történt az incidens, milyen rendszert/adathordozót érintően, milyen körben és milyen mennyiségben voltak érintve személyes adatok, mikor és hogyan fedezték fel az incidenst, incidens oka),

b) adatvédelmi incidens hatásai, következményei, lehetséges kockázatok,

c) adatvédelmi incidens orvoslásának módja, az e körben tett intézkedések leírása.

**23. §** (1) Amennyiben a kivizsgálás eredményeként megállapítható, hogy az érintettre nézve kockázatot jelentő adatvédelmi incidens következett be, annak bejelentését az az információbiztonsági felelős javaslatára az adatvédelmi tisztviselő végzi el a Nemzeti Adatvédelmi és Információszabadság Hatóság által ezen célra rendszeresített módon, a lehető legrövidebb idő alatt, de legkésőbb 72 órával az incidens bekövetkezésének tudomásra jutásától.

(2) Amennyiben az incidens valószínűsíthetően magas kockázattal jár, az érintettek adatvédelmi incidensekről történő tájékoztatását az adatvédelmi tisztviselő haladéktalanul kezdeményezi az érintetti körtől függően kialakított formában és tartalommal, az adatkezelés jellegétől és céljától függően a hitelezési és ügyfélkapcsolati igazgató, valamint a marketing és kommunikációs igazgató bevonásával.

(3) Nem szükséges az érintetteket tájékoztatni az incidensről, ha a GDPR 34. cikk (3) bekezdésében meghatározott valamely feltétel fennállása megállapítható:

a) az adatkezelő előzetesen megfelelő technikai intézkedéseket alkalmazott (pl. titkosítás), így a jogosultatlanul megszerzett vagy hozzáférhetővé vált adat nem értelmezhető;

b) további intézkedések megtételére került sor, ezért az incidens eredményeként megállapítható magas kockázat valószínűleg nem valósul meg (pl. távoli eléréssel adattörlés);

c) a tájékoztatás aránytalan erőfeszítéssel járna, ezért egyedi tájékoztatás helyett elegendő közleményt közzétenni.

# V. FEJEZET
# AZ ÉRINTETTI JOGOK GYAKORLÁSÁNAK ELŐSEGÍTÉSE

## Adatvédelmi bejelentések, kifogások, érintetti kérelmek kezelése

**24. §** (1) Amennyiben valamely érintett a GDPR 14-22. cikkeiben meghatározott jogosultságával élve kérelmet nyújt be a DHK Zrt-hez, azt ügyfél esetében a hitelezési és ügyfélkapcsolati igazgató, munkavállaló esetén a HR vezető, hírlevél-küldés, promóciós játék, közérdekű adatigénylés vagy honlap-látogatás esetén a marketing és kommunikációs igazgató, üzleti partner kapcsolattartója esetén az érintett szerződés tárgya szerint illetékes szervezeti egység vezetője – vagy az ezen vezetők által kijelölt munkavállaló - vizsgálja ki. A kivizsgálásba az adatvédelmi tisztviselőt minden esetben be kell vonni.

(2) Az érintett kérelme alapján indult vizsgálat eredményeként az adatvédelmi tisztviselő véleményét figyelembe véve a kivizsgálást végrehajtó vezető vagy munkavállaló legfeljebb egy hónapon belül gondoskodik a kérelem teljesítéséről vagy elutasításáról és az érintett erről való tájékoztatásáról. A tájékoztatásnak ki kell terjednie a felügyeleti hatóságnál történő panasz benyújtásának, valamint a bírósági jogorvoslat kezdeményezésének lehetőségére.

## Adatkezelési folyamatok fejlesztése

**25. §** Amennyiben az adatvédelmi tisztviselő az általa lefolytatott adatvédelmi audit, vagy az érintetti kérelem alapján arra a következtetésre jut, hogy az adatkezelés köre, időtartama vagy módszere módosítást igényel, az adatkezeléssel érintett szakterület(ek) vezetőinek bevonásával részletes indokolással és javaslattal ezek módosítását kezdeményezi, továbbá jogosult célzott adatvédelmi tudatosság-növelő belső oktatást szervezni.