MAGYAR CORVIN-LÁNC TESTÜLET

Magyar Corvin-lánc Testület
Adatvédelmi szabályzat

(változásokkal egységes szerkezetbe foglalt)

2023.

A Magyar Corvin-lánc Testület (a továbbiakban: Testület) a 2019. május 10. napján megtartott közgyűlésén 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 szóló, az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) (a továbbiakban: GDPR), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) foglalt kötelezettsége alapján a Testület által kezelt személyes adatok védelme érdekében elfogadott szabályzatának szövegét a .../2023. (XI.6.) számú közgyűlési határozattal – változásokkal egységes szerkezetben – az alábbiak szerint fogadja el.

ÁLTALÁNOS RÉSZ

I. A Szabályzat célja és hatálya

1. A Szabályzat célja, hogy meghatározza a Testület tevékenysége és működése során általa kezelt természetes személyek személyes adatainak védelmére irányuló intézkedések és eljárások jogszerű rendjét, valamint biztosítsa az adatvédelem alapjogi elveinek, az információs önrendelkezési jognak, a személyes adatok védelméhez való jognak és az adatbiztonság követelményeinek érvényesülését.

2. A Szabályzat személyi hatálya kiterjed

   a) a Testület valamennyi szervezeti egységére, és a Testületnél munkaviszony, megbízási jogviszony, vagy egyéb munkavégzésre irányuló jogviszony alapján munkát végző természetes személyre, aki tevékenysége során személyes adatot kezel;

   b) minden, a Testület szolgáltatásait vagy szervezeti egységeit, infrastruktúráját igénybe vevő, vagy a Testülettel akár jogviszony létesítése céljából, akár egyéb célból ténylegesen kapcsolatba került, vagy kerülő természetes személyre;

   c) azon személyekre is, akik a Testülettel nem állnak az a)-b) pont szerinti jogviszonyban, illetve kapcsolatban, azonban személyes adataikat jogszabályi előírás folytán a Testület kezeli;

   d) a Testület által adatfeldolgozóként igénybe vett szerződött partnerek adatfeldolgozást végző munkavállalóira;

   e) a Testülettel szerződött partneri viszonyban álló szolgáltatók munkavállalóira.

3. A Szabályzat tárgyi hatálya kiterjed a Testület által bármely célból kezelt személyes adatra és a személyes adatoknak a Testületnél megtalálható valamennyi nyilvántartására, függetlenül azok megjelenési formájától.

4. A Szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az információbiztonsági szabályzat rendelkezik.

II. A Szabályzat alkalmazásában használt fogalmak

5. A Szabályzat alkalmazása során a fogalmak az alábbiak szerint értelmezendők:

   a) Személyazonosító adatok: a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, személyi igazolvány száma (a továbbiakban: szem. ig. szám), valamint személyi azonosító szám

együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet a természetes személy azonosítására.

b) 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. Jelen Szabályzat alkalmazásában valamennyi „adat" megjelölés alatt a személyes adatok értendők.

c) Különleges adat: a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

d) Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése vagy az adatokba való betekintés.

e) Adatkezelő: a Testület, továbbá az a természetes vagy jogi személy, közhatalmi szerv, illetve jogi személyiséggel nem rendelkező bármely szervezet, aki, vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

f) Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

g) 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.

h) Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

i) Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

j) Adattovábbítás: az adatnak egy meghatározott harmadik személy számára történő hozzáférhetővé tétele.

k) Adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

l) Felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság.

m) 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 előre jelzésére használnak.

n) 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;

o) 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;

p) 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.

III. Adatkezelők és adatfeldolgozás

6. A Testülettel jogviszonyban álló valamennyi személy, aki személyes adat birtokába jut, ilyet munkaköre vagy tisztsége alapján kezel, köteles védeni és őrizni a személyes adatokat, és minden erőfeszítést megtenni annak érdekében, hogy azoknak megfelelő védelmét biztosítsa.

7. Az adatokat védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

8. A Testülettel jogviszonyban állók, illetve a Testület képviseletében eljáró személyek kötelesek bizalmasan kezelni minden olyan személyes adatot, amely előttük a jogviszonyukkal összefüggésben vált ismertté.

9. A Testülettel jogviszonyban álló adatkezelést vagy adatfeldolgozást végző személyek felelősséggel tartoznak minden olyan kárért, amely adatkezelési és adatvédelmi kötelezettségük megszegéséből származik.

10. Amennyiben az adatkezelést a Testület nevében más végzi, a Testület kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

11. Az adatfeldolgozó által végzett adatkezelést olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót a Testülettel szemben. A szerződés kizárólag írásban köthető meg, és abban a GDPR 28. cikk (3) bekezdésében rögzített tartalmat is rögzíteni szükséges, így különösen azt, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza az adatkezelés biztonsága érdekében szükséges, a GDPR 32. cikkében előírt intézkedéseket;

d) a további adatfeldolgozó igénybevételére vonatkozóan tiszteletben tartja a GDPR 28. cikk (2) és (4) bekezdésben említett feltételeket;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett GDPR III. fejezetében foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségeinek – így elsősorban az adatvédelmi incidens bejelentése, az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció - teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely a fenti kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Az adatfeldolgozó köteles haladéktalanul tájékoztatni az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti a GDPR vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

12. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.

13. Amennyiben szükséges, az adatkezelő és az adatfeldolgozó további intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat.

IV. Az érintett hozzájárulása, mint az adatkezelés jogalapja

14. Amennyiben az adatkezelés jogalapja az érintett hozzájárulása, úgy a Testületnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez megfelelően hozzájárult.

15. Az „érintett hozzájárulása" akkor tekinthető az adatkezelés érvényes jogalapjának, amennyiben az 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. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

16. Az érintett hozzájárulása során biztosítani kell azt, hogy valódi választási lehetőség álljon az érintett rendelkezésére. Nem minősül önkéntesnek a hozzájárulás akkor, ha az érintettnek nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, ha ez kárára válna, továbbá ha az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn.

17. Nem tekinthető önkéntesnek a beleegyezés, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez.

18. Nem tekinthető önkéntesnek a hozzájárulás, ha a szerződés teljesítését (például a szolgáltatás nyújtását) olyan adatkezeléshez való hozzájárulásához kötik, amely adatkezelés nem szükséges a szerződés teljesítéséhez.

19. Az adatkezelőnek biztosítania kell, hogy az érintett a hozzájárulását bármikor visszavonhassa. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló adatkezelés jogszerűségét a visszavonást megelő időszak tekintetében. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

20. Amennyiben az adatkezelő írásbeli nyilatkozaton keresztül szerzi be az érintett hozzájárulását, akkor a nyomtatványon a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani a szerződés többi részétől, valamint ezen kérelmet érthető és egyszerű nyelvezettel kell az adatkezelőnek megfogalmaznia.

V. Az érintett jogai és azok érvényesítése

A) Tájékoztatási kötelezettség

21. Amennyiben a kezelt személyes adatokat a Testület az érintettől szerzi be, az érintettek részére a személyes adatok megszerzésének időpontjában tájékoztatást kell adni az adatkezelő és képviselőjének kilétéről és elérhetőségéről, a Testület adatvédelmi tisztviselőjének elérhetőségéről, a személyes adatok tervezett kezelésének céljáról, jogalapjáról, jogos érdeken alapuló adatkezelés esetén az adatkezelő vagy harmadik fél jogos érdekéről, a személyes adatok címzettjeiről, illetve a címzettek kategóriáiról, harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás tényéről, az adatok tárolásának időtartamáról vagy az időtartam meghatározásának szempontjairól, az érintett azon jogáról, hogy kérheti a Testülettől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról, arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása, adott esetben az automatizált döntéshozatal és profilalkotás tényéről. A tiltakozáshoz való jog érvényesítésének lehetőségéről való tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

22. A fenti tájékoztatást

    a) a Testülettel munkaviszonyt, megbízási vagy más munkavégzésre irányuló egyéb jogviszonyt létesítő személyek részére a jogviszony létrejöttekor, az általános tájékoztatást a Testület vonatkozó adatkezelési tájékoztatója szerinti tartalommal;

b) a Testülettel szerződéses jogviszonyban álló személyek számára a Testület vonatkozó adatkezelési tájékoztatója szerinti tartalommal

kell megadni.

Az a) pont szerinti tájékoztatást papír alapon, elektronikusan vagy a szerződés szövegébe építve, a b) pont szerinti tájékoztatást akként kell megadni, hogy a szerződés szövegébe építve utalni kell a kapcsolódó adatkezelési tájékoztató elérhetőségére.

Annak érdekében, hogy a Testülethez álláspályázatot benyújtók számára a személyes adataik kezelésével kapcsolatos adatkezelési tájékoztató már az álláspályázat benyújtását megelőzően megismerhető legyen, a Testület az álláspályázati felhívásban utal a kapcsolódó adatkezelési tájékoztató honlapon való elérhetőségére.

23. Amennyiben a kezelt személyes adatokat a Testület nem az érintettől szerzi be, akkor a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb 1 hónapon belül, ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával, vagy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor megadja az érintettek számára a szükséges tájékoztatást. Ennek keretében az érintetteket tájékoztatni kell a Testület és képviselőjének kilétéről és elérhetőségéről, az adatvédelmi tisztviselő elérhetőségéről, a személyes adatok tervezett kezelésének céljáról, valamint az adatkezelés jogalapjáról, az érintett személyes adatok kategóriáiról, a személyes adatok címzettjeiről, illetve a címzettek kategóriáiról, annak tényéről, hogy valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére adattovábbításra sor kerül-e, a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól, jogos érdeken alapuló adatkezelés esetén az adatkezelő vagy harmadik fél jogos érdekéről, az érintett azon jogáról, hogy kérheti a Testülettől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról, hozzájáruláson alapuló adatkezelés esetén az érintett azon jogáról, hogy a hozzájárulását bármikor visszavonhatja, ez azonban nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét, a felügyeleti hatósághoz címzett panasz benyújtásának jogáról, a személyes adatok forrásáról és adott esetben arról, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e, adott esetben az automatizált döntéshozatal, illetve a profilalkotás tényéről.

24. A Testület a 22. pontban nem rögzített, egyéb személyes adatkezeléssel járó tevékenységeihez kapcsolódó tájékoztatásokat – annak érdekében, hogy azok az érintettek számára előzetesen megismerhetők legyen – a honlapján e célra létrehozott, „Adatvédelem" fül alatt teszi közzé tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva.

25. Nem magyar anyanyelvű személy esetében a tájékoztatást az anyanyelvén is meg kell adni. Ebben az esetben a tájékoztatás fordításáról a Testület adatvédelmi tisztviselője gondoskodik.

26. A Testület minden olyan címzettet tájékoztat a személyes adatot érintő valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

B) Az érintett tájékoztatáshoz való joga (hozzáféréshez való jog)

27. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő a kérelem beérkezésétől számított

legkésőbb 1 hónapon belül tájékoztatást ad az érintett vonatkozásában folyamatban lévő adatkezelésről.

28. Az érintett jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

e) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;

f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

h) automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

29. A személyes adatokhoz való hozzáférést úgy kell biztosítani, hogy ez alatt az érintett más személy adatait ne ismerhesse meg.

30. Az érintett hozzáféréshez való jogát a Testület az elérni kívánt céllal arányosan korlátozhatja vagy megtagadhatja, ha ezen intézkedés elengedhetetlenül szükséges:

a) a Testület részvételével végzett vizsgálatok vagy eljárások – így különösen büntetőeljárás – hatékony és eredményes lefolytatásának;

b) bűncselekmények hatékony és eredményes megelőzésének és felderítésének;

c) bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának;

d) a közbiztonság hatékony és eredményes védelmének;

e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen honvédelem és nemzetbiztonság; vagy

f) harmadik személyek alapvető jogai védelmének biztosításához.

31. Amennyiben a Testület a megtagadja vagy korlátozza az érintett hozzáférési jogát, erről haladéktalanul írásban tájékoztatja érintettet – amennyiben a korlátozás, megtagadás célját ez nem veszélyezteti – az intézkedés indokát is megjelölve. A tájékoztatásban Testület külön felhívja az érintett figyelmét, hogy hozzáférési jogát a felügyeleti hatóság közreműködésével is gyakorolhatja.

C) A helyesbítéshez való jog

32. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül helyesbíti

az érintettre vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

D) Az adatkezelés korlátozásához való jog

33. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő korlátozza az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

    a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő ellenőrizze a személyes adatok pontosságát;

    b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

    c) a Testületnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

    d) az érintett tiltakozási jogával élt az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

34. Amennyiben az adatkezelés a fentiek szerinti korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

35. Az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

E) A törléshez való jog

36. Az érintett – jogosultsága igazolását követően befogadott – kérelmére az adatkezelést végző illetékes ügyintéző vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül törli az érintett személyes adatait vagy azoknak az érintett által meghatározott körét, feltéve, hogy az alábbi esetek valamelyike fennáll:

    a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

    b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;

    c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;

    d) a személyes adatokat jogellenesen kezelték;

    e) a személyes adatokat a Testületre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

    f) a személyes adatok gyűjtésére a közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor;

37. Amennyiben a Testület nyilvánosságra hozta a személyes adatot, és azt a fentiek szerint törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével

megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlése érdekében.

38. A Testület a személyes adatok törlését a jogszerű kérelem ellenére sem végezheti el, amennyiben az adatkezelés szükséges:

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) a személyes adatok kezelését előíró, a Testületre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése céljából;

c) közérdekből végzett feladat végrehajtása céljából;

d) közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az adattörlés valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést;

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

F) A tiltakozáshoz való jog

39. Amennyiben a Testület az érintett adatait az alábbi jogalapokon kezeli:

a) az adatkezelés közérdekű feladat végrehajtásához szükséges; vagy

b) az adatkezelés a Testület vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,

az érintett az így kezelt személyes adatok kezelése ellen tiltakozhat, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben a Testület a személyes adatokat nem kezelheti tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

40. Amennyiben a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

G) Jogorvoslathoz való jog

41. Az adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett – az adatkezelést végző ügyintéző útján vagy közvetlenül – az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja, és ha alapos, a Testület főtitkáránál intézkedést kezdeményez, ellenkező esetben a panaszt elutasítja. Az elutasításról a panaszost a kérelem kézhezvételét követő legkésőbb 1 hónapon n belül írásban tájékoztatja, a kérelem elutasításának ténybeli és jogi indokait is közölve. A kérelem elutasítása esetén a panaszost tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti szervhez fordulás lehetőségéről is. Az elutasított kérelmekről az adatvédelmi tisztviselő jegyzőkönyvet köteles felvenni.

VI. Az adatkezelés biztonsága

A) Adatbiztonsági szabályok

42. Az adatbiztonság érdekében a Testület felméri és nyilvántartja az általa végzett valamennyi adatkezelési tevékenységet. A nyilvántartást az adatvédelmi tisztviselő vezeti.

43. Az adatkezelési tevékenységek nyilvántartása alapján a Testület kockázatelemzést végez annak felmérése érdekében, hogy az egyes adatkezelés mely szervezeti egysége által, milyen feltételek szerint valósul meg, illetve az adatkezelés során mely kockázati tényezők milyen mértékű sérelmet, milyen lehetséges adatvédelmi incidenst okozhatnak. A kockázatelemzést a ténylegesen megvalósuló adatkezelési tevékenység alapján kell elvégezni. A kockázatelemzés célja olyan biztonsági szabályok, valamint intézkedések meghatározása, amelyek a Testület működéséhez, tevékenységéhez igazodva hatékonyan biztosítják a személyes adatok megfelelő védelmét.

44. A Testület az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik - ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

45. A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

46. Ezen intézkedéseket az adatvédelmi tisztviselő felülvizsgálja és szükség esetén naprakésszé teszi.

47. A Testület 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. Ezen intézkedéseknek különösen azt kell biztosítaniuk, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

48. Személyes adatot tartalmazó irat nem hagyható olyan helyen, ahol harmadik személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban, illetve személyzeti helyiségekben is gondoskodni kell, ahol az illetékes iratkezelőkön kívül más, harmadik személy is megfordulhat.

49. Az adathordozó képek és dokumentációk elhelyezésének-, fizikai védelmének biztonságáról az adatkezelő szervezeti egység vezetője az adatvédelmi tisztviselővel egyetértésben dönt.

50. A szervezeti egységeknél kialakítandó adatkezelési rendszer környezetének védelméről a helyi adottságok figyelembevételével az illetékes vezetőknek kell gondoskodni, beleértve az adatsértések megelőzését is.

51. A manuálisan kezelt személyes adatok elvesztésének megelőzése érdekében eredeti iratokat csak hivatalos ügyintézés, különösen bírósági eljárás vagy nyomozati eljárás során lehet kiadni. Kiadást megelőzően az eredeti iratokról az illetékes szervezeti egységnél történő megőrzés céljára hiánytalan másolatot kell készíteni.

52. Személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló egyéb adatforrásokból meg kell kísérelni a lehetséges mértékig a károsodott adatok pótlását. A sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. Az adatpótlásba be kell vonni azon illetékes adatkezelő személyt, aki az adatok rögzítésében közreműködött. A pótolt adatokon a pótlás tényét fel kell tüntetni.

B) Adatvédelmi tisztviselő

53. Az adatvédelmi tisztviselőt az elnök bízza meg és az elnöknek tartozik felelősséggel.

54. Az adatvédelmi tisztviselő a Testület alkalmazottja lehet, vagy szolgáltatási szerződés keretében láthatja el a feladatait. Kinevezése során a szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR 39. cikkében említett feladatok ellátására való alkalmasságra szükséges figyelemmel lenni.

55. Kinevezését követően a Testület honlapján közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatósággal közli.

56. Az adatvédelmi tisztviselő ellátja a GDPR által nevesített feladatait, e tekintetben köteles szorosan együttműködni a Testület szervezeti egységeivel és a főtitkárral.

57. Az adatvédelmi tisztviselő feladatai különösen:

    a) tájékoztat és szakmai tanácsot ad a Testületnél az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

    b) ellenőrzi az GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek való megfelelést továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

    c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;

    d) együttműködik a felügyeleti hatósággal;

    e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele;

    f) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

    g) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az illetékes adatkezelőt vagy az adatfeldolgozót;

    h) gondoskodik az adatvédelmi ismeretek Testületnél történő oktatásáról.

58. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

59. Az adatvédelmi tisztviselő nyilvántartást vezet:

a) a Testületnél végzett adatkezelési tevékenységekről. A nyilvántartás tartalmazza az adatkezelő szervezeti egység nevét és elérhetőségét, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a nevét és elérhetőségét; az adatkezelés céljait; az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését; olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat (beleértve a megfelelő garanciák leírását), ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidőket; és ha lehetséges, az adatvédelmi biztonsági technikai és szervezési intézkedések általános leírását. A nyilvántartást írásban vagy elektronikus formában kell megőrizni, és folyamatosan naprakészen tartani.

b) a Testületnél észlelt adatvédelmi incidensekről. A nyilvántartás az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a jelen szabályzat 2. sz. mellékletében meghatározottak szerint.

c) a Testületnél végzett adattovábbításról. Az adattovábbítási nyilvántartás az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából tartalmazza a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat a jelen szabályzat 3. sz. mellékletében meghatározottak szerint.

60. Az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódhat, feladatai ellátása során a személyes adatokhoz és az adatkezelési műveletekhez hozzáférhet.

61. Az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban nem utasítható.

62. A Testület az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.

63. Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

64. Az adatvédelmi tisztviselő feladatai ellátása során a teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

65. Az adatvédelmi tisztviselő más feladatokat is elláthat. Amennyiben a Testület az adatvédelmi tisztviselőt más feladatokkal is megbízza, abban az esetben biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

C) Adatvédelmi hatásvizsgálat és előzetes konzultáció

66. Amennyiben 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 a Testület 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.

67. A Testület az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.

68. Az adatvédelmi hatásvizsgálatot 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 személyes adatok különleges kategóriái, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy

c) nyilvános helyek nagymértékű, módszeres megfigyelése.

69. A hatásvizsgálat kiterjed legalább:

a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;

c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

70. A Testület – a kereskedelmi érdekek vagy a közérdek védelmének vagy az adatkezelési műveletek biztonságának sérelme nélkül – kikérheti az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.

71. A Testület szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése a korábban lefolytatott adatvédelmi hatásvizsgálatnak megfelelően történik-e.

72. Amennyiben 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 adatvédelmi felelős konzultál a felügyeleti hatósággal (előzetes konzultáció).

73. A Testület az adatvédelmi tisztviselő útján a felügyeleti hatósággal folytatott előzetes konzultáció során a felügyeleti hatóságot tájékoztatja:

a) adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;

b) a tervezett adatkezelés céljairól és módjairól;

c) az érintettek e rendelet értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;

d) az adatvédelmi hatásvizsgálatról; és

e) a felügyeleti hatóság által kért minden egyéb információról.

D) Adatvédelmi incidens kezelése

74. Amennyiben a Testület bármely munkavállalója, megbízottja, illetve a Testület nevében egyéb jogcímen eljárni jogosult személy adatvédelmi incidens megtörténtét észleli, vagy arról szerez tudomást, azt haladéktalanul jeleznie kell az adatvédelmi tisztviselő számára a jelen szabályzat 1. mellékletében található adatvédelmi incidens bejelentő lap kitöltése mellett.

75. Az adatvédelmi incidenst az adatvédelmi tisztviselő indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidens észlelésre került, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, a bejelentéshez mellékelni kell a késedelem igazolására szolgáló indokokat is.

76. A felügyeleti hatóság felé történő bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell a Testület által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

77. Amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

78. Az adatvédelmi tisztviselő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

79. Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Testület – elsősorban az adatvédelmi tisztviselő útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

80. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következő információkat és intézkedéseket:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) a Testület által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

81. Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) a Testület megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása

–, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) a Testület az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

82. Az adatvédelmi incidensre tekintettel meghozott intézkedések végrehajtását követően a Testület felméri az intézkedések hatékonyságát, szükség esetén az érintett adatkörben újabb kockázatelemzést végez.

VII. Adattovábbítás

83. A Testület szervezeti rendszerén belül a személyes adatok – a feladat elvégzéséhez szükséges mértékben és ideig – olyan szervezeti egységhez, személyhez továbbíthatók, amelynek a Testületnél végzett feladata ellátásához a személyes adatok megismerése és kezelése szükséges.

84. A Testületnél különböző célra irányuló adatkezelések csak törvényes céloknak megfelelően, indokolt esetben kapcsolhatók össze.

85. Olyan megkeresés, amely a Testület által kezelt személyes adat továbbítására irányul, csak jogszabályi előírás alapján vagy ennek hiányában kizárólag olyan esetben teljesíthető, ha az érintett ehhez – részletes tájékoztatást követően – igazolható módon hozzájárul. Minden más esetben az adattovábbítás teljesítését meg kell tagadni.

86. Külföldre irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban előírt feltételei fennállnak-e. Ennek kapcsán vizsgálandó, hogy az adattovábbítás a GDPR-ban meghatározott valamely jogalapnak megfelelően történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e. Amennyiben az adattovábbítás az Európai Gazdasági Térség valamely tagállamába irányul, úgy a személyes adatok megfelelő szintű védelmét nem kell vizsgálni.

87. Olyan személyes adatok továbbítására – ideértve a személyes adatok harmadik országból vagy nemzetközi szervezettől egy további harmadik országba vagy további nemzetközi szervezet részére történő újbóli továbbítását is –, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, ha az adatkezelő és az adatfeldolgozó egyaránt teljesíti a GDPR-ban rögzített feltételeket.

88. Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására sor kerülhet, ha az Európai Bizottság megállapította, illetve az Európai Unió Hivatalos Lapjában és annak honlapján közzétette, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít (megfelelőségi határozat). Az ilyen adattovábbításhoz nem szükséges külön engedély.

89. Személyes adatok továbbítása során, amennyiben az postai küldeményként történik, a küldeményt zártan kell feladni.

90. A Testület vállalja, hogy a személyes adatokat statisztikai célra kizárólag olyan módon adja át, hogy azokat az érintettel ne lehessen kapcsolatba hozni.

KÜLÖNÖS RÉSZ

VIII. Manuálisan kezelt személyes adatok

91. A Testületnek az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választania, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Testületnek.

92. A manuálisan kezelt személyes adatok biztonsága érdekében az alábbi intézkedéseket kell foganatosítani:

    a) az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni;

    b) a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi iratokat biztonságosan elzárva kell tartani,

    c) a Testület által végzett adatkezelések iratainak archiválását rendszeresen el kell végezni, az archivált iratokat a Testület iratkezelési és selejtezési szabályzatának, valamint az irattári tervének megfelelően kell szétválogatni és irattári kezelésbe venni, figyelemmel a köziratokról, a közleveltárakról és a magánleveltári anyag védelméről szóló 1995. évi LXVI. törvény és a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet előírásaira is.

93. Az érintett helyiségek, illetve szekrények kulcsához való hozzáférés rendjét a Testület illetékes szervezeti egységének vezetője állapítja meg, melyet az adatvédelmi tisztviselő részére köteles tájékoztatásul megküldeni.

IX. Elektronikusan kezelt személyes adatok

94. Amennyiben a Testület olyan elektronikus rendszerben kezel személyes adatot, amelybe csak a hozzáférési listára felvett, nyilvántartott, arra illetékes személy léphet be, úgy az arra illetékesnek egyéni, titkos jelszóval kell bejelentkeznie a rendszerbe, mely egyéni jelszó védelméről – az adatvédelmi incidensek elkerülése végett is – az arra illetékes gondoskodni köteles, továbbá az adatkezelés befejeztével a rendszerből ki kell lépnie. Az arra illetékes számára kiosztott egyéni jelszó rajta kívül kizárólag az adatkezelési szoftver fejlesztését, üzemeltetését ellátó informatikai munkatársak, valamint az adatvédelmi tisztviselő által ismerhető meg, ha az a Testületnél elvégzendő feladatuk ellátásához szükségessé válik.

95. Az adatkezelésre használt számítógépek adatbevitelre, lekérdezésre alkalmas állapotban történő, felügyelet nélkül hagyása tilos.

96. A Testület kizárólag olyan adatkezelési rendszert alkalmazhat, amely a rendszerbe történt belépést regisztrálja, illetve a rögzített adatokról megállapítható, hogy az adatrögzítés ki által és milyen időpontban történt.

X. Testületi tagok adatainak kezelése

97. A Testületi tagok személyes adatait a Testület a GDPR-ban és az Infotv.-ben rögzített garanciák maradéktalan betartása mellett, a vonatkozó jogszabályban meghatározottak szerint kezeli.

ZÁRÓ RENDELKEZÉSEK

98. Jelen Szabályzatot a Testület valamennyi szervezeti egysége számára folyamatosan hozzáférhetővé kell tenni.

99. Jelen Szabályzat mellékleteinek módosítására a főtitkár jogosult, az a jelen Szabályzat közgyűlés általi formális módosítását nem igényli.

100. Jelen Szabályzatot elfogadását követően a Testület honlapján nyilvánosan elérhetővé kell tenni.

101. Jelen Szabályzat a Magyar Corvin-lánc Testület Közgyűlése általi elfogadásának napján lép hatályba és visszavonásig hatályos.

Budapest, 2023.november 6.

Prof. Dr. Vizi E. Szilveszter	Dr. Klinghammer István
elnök	főtitkár

MELLÉKLETEK

1. sz. melléklet

Adatvédelmi incidens bejelentőlap

Kérjük a tudomásszerzést követően haladéktalanul kitölteni, és a Magyar Corvin-lánc Testület adatvédelmi tisztviselőjéhez eljuttatni!

I. Adatvédelmi incidensről tudomást szerző munkatárs

- neve:
- beosztása:
- munkahelyi elérhetősége:

II. Az adatvédelmi incidens

- jellege:
- feltételezett időpontja, helye:
- által érintett személyek kategóriái és hozzávetőleges száma:
- által érintett személyes adatok köre és hozzávetőleges száma:
- észlelt vagy lehetséges következményei:
- orvoslására tett vagy tervezett intézkedés és az intézkedés elrendelője valamint végrehajtója (név és beosztás szerint):

III. Az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve: IGEN / NEM

IV. Egyéb észrevétel:

Budapest, 20.... (év) ..... (hó). .....(nap)

2. sz. melléklet

Adatvédelmi incidens nyilvántartás

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 szóló, az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) (GDPR) 33. cikk (5) bekezdésének való megfelelés, valamint a GDPR 5. cikk (2) bekezdésében foglalt elszámolhatóság érvényesítése érdekében a Magyar Corvin-lánc Testület az alábbi nyilvántartást vezeti az adatvédelmi incidensekről.

#	Az adatvédelmi incidens időpontja, helye	Az adatvédelmi incidenssel érintettek köre, száma	Az érintett személyes adatok köre	GDPR 9. cikk, vagy 10. cikk szerinti adatot érint	Harmadik országba továbbítás történt	Az adatvédelmi incidens körülményei, az adatkezelést előíró jogszabályban meghatározott egyéb adatok	Az adatvédelmi incidens hatásai	Az adatvédelmi incidens elhárítására megtett intézkedések	Bejegyzés dátuma, bejegyző neve, aláírása
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									

3. sz. melléklet

Adattovábbítási nyilvántartás

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 szóló, az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) (GDPR) preambulumának (111) bekezdésében foglalt elvárások teljesítésének ellenőrizhetősége, a GDPR 5. cikk (2) bekezdésében foglalt elszámolhatóság érvényesítése érdekében a Magyar Corvin-lánc Testület az alábbi adattovábbítási nyilvántartást vezeti.

#	Személyes adatok továbbításának időpontja	Az adatszolgáltatást teljesítő szervezeti egység megnevezése	Az adattovábbítás jogalapja és célja	A továbbított személyes adatok körének meghatározása	Az adattovábbítás címzettje	Harmadik országba történt adattovábbítás	Az adatkezelést előíró jogszabályban meghatározott egyéb adatok, további megjegyzés	Bejegyzés dátuma, bejegyző neve, aláírása
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								