Az Alkotmánybíróság elnökének 4/2026. (III. 23.) utasítása az Alkotmánybíróság adatvédelmi és adatbiztonsági szabályzatáról

1.Általános rendelkezések

1. Az adatvédelmi és adatbiztonsági szabályzat célja, hatálya

1.1. Az adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza az Alkotmánybíróságnál, illetve az Alkotmánybíróság Hivatalánál (a továbbiakban: Hivatal) (a továbbiakban együtt: Alkotmánybíróság) folytatott személyes adatok kezelésének jogszerű rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését.
1.2. A Szabályzat célja az 1.1. pontban foglaltakon túl az Alkotmánybíróság által lefolytatott eljárások során az érintettek személyes adatai védelmének biztosítása.
1.3. A Szabályzat hatálya kiterjed az Alkotmánybíróság tagjaira és a Hivatal által foglalkoztatott valamennyi köztisztviselőre és munkavállalóra, valamint ösztöndíjat elnyert személyekre (a továbbiakban együtt: foglalkoztatott), továbbá azon személyekre, akik szakmai gyakorlat keretében az Alkotmánybíróságnál személyes adatokat ismernek meg.
1.4. Az Alkotmánybírósághoz beérkező és az Alkotmánybíróságnál keletkezett iratok készítésének, kezelésének, nyilvántartásának, irattározásának és selejtezésének alapvetői szabályait, az iratkezeléssel összefüggő adatvédelmi és adatbiztonsági szabályokat az Alkotmánybíróság mindenkor hatályos iratkezelési szabályzatával és irattári tervével összhangban kell alkalmazni.
1.5. A Hivatal elektronikus információs rendszereiben tárolt személyes adatok védelmére vonatkozóan a Szabályzat rendelkezéseit az Alkotmánybíróság Hivatalának informatikai biztonsági szabályzatában foglaltakkal összhangban kell alkalmazni.
1.6. A Szabályzatot a minősített adatokat tartalmazó iratok (TÜK-iratok) tekintetében az Alkotmánybíróság Hivatalának a minősített adatok védelmére vonatkozó biztonsági szabályzatában meghatározottakkal összhangban kell alkalmazni.
1.7. A Szabályzatot az Európai Parlament és a Tanács (EU) 2016/679 Rendeletére (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 2. § (2) bekezdése szerint azt kiegészítő előírásokra figyelemmel, továbbá az alkalmazandó ágazati jogszabályi követelményekkel összhangban kell alkalmazni.
1.8. A Szabályzatban alkalmazott fogalmak tekintetében az általános adatvédelmi rendelet 4. cikke szerinti meghatározások az irányadók.

2.Az Alkotmánybíróság adatvédelmi rendszere

2.1. A személyes adatok kezelésével kapcsolatos felelősségek

2.1.1. A személyes adatok védelméért, az adatkezelés jogszerűségéért az Alkotmánybíróság elnöke (a továbbiakban: elnök) felel.
2.1.2. A személyes adatok védelme és az adatkezelés jogszerűsége érdekében az elnök:

a) szabályzatok és kötelező utasítások 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;
b) gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról, az adatvédelmi és adatbiztonsági intézményrendszer működtetéséről, a működéshez szükséges intézkedések megtételéről;
c) meghozza az Alkotmánybíróság mint adatkezelő tekintetében az adatkezelésre vonatkozó döntéseket;
d) írásban kijelöli az Alkotmánybíróság adatvédelmi tisztviselőjét a GDPR 37. cikk (5) bekezdése alapján;
e) a főtitkár útján felel az Alkotmánybíróság adatkezelési tevékenységével kapcsolatos közzétételi kötelezettség teljesítéséért.
2.1.3. Az elnök az adatkezelés személyi és tárgyi feltételeinek biztosításáról, a szabályzatban foglaltak végrehajtásáról, az adatvédelemmel kapcsolatos szabályok foglalkoztatottak általi megismeréséről és betartásáról a főtitkár és a gazdasági főigazgató útján gondoskodik.
2.1.4. Az elnök az adatkezeléssel kapcsolatos döntések előkészítését, az elszámoltathatóság érdekében szükséges dokumentáció és intézkedések tervezetének összeállítását a főtitkár és a gazdasági főigazgató útján végzi.
2.1.5. A főtitkár
a) dönt a szükséges hozzáférési jogosultságok kiadásáról és visszavonásáról ;
b) gondoskodik az adatvédelmi követelmények érvényre juttatásáról;
c) intézkedik a Szabályzatban vagy más kötelező erejű adatvédelmi előírásban foglaltak ellenőrzéséről, azok megsértése esetén a hiányosságok haladéktalan felszámolásáról.
2.1.6. A foglalkoztatottak
a) a Szabályzatban meghatározottak szerint kezelik a feladataik ellátásával összefüggésben tudomásukra jutott személyes adatokat;
b) betartják az adatkezelésre vonatkozó jogszabályokban és belső szabályzatokban foglalt előírásokat;
c) tudásukat naprakészen tartják a munkavégzésükre irányadó adatvédelmi és adatbiztonsági előírások kapcsán és az adatvédelmi incidensek gyanújának felismerése érdekében.
2.1.7. Az Alkotmánybíróságnál adatkezelést végző foglalkoztatott fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a feladat- és hatáskörének gyakorlása során tudomására jutott személyes adatok jogszerű kezeléséért, az Alkotmánybíróság nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.
2.1.8. Az adatvédelemmel összefüggő számítógépes adatkezelés szabályairól, így különösen az archiválás, mentés, törlés rendjéről, továbbá az egyes programok és belső tárhelyek tekintetében a hozzáférési és a betekintési jogosultságokról és az ehhez kapcsolódó ügyintézői hozzáférésekről az Alkotmánybíróság informatikai biztonsági szabályzata rendelkezik.

2.2. Az Alkotmánybíróság szervezetén kívüli személyek bevonása az adatkezelés folyamatába

2.2.1. Amennyiben az elnök döntése alapján az Alkotmánybíróság közfeladatának ellátása érdekében adatfeldolgozó igénybevétele szükséges, úgy az általános adatvédelmi rendelet 28. cikke szerinti tartalommal az adatfeldolgozó felelősségét önálló szerződésben vagy a felek között létrejövő őszolgáltatási szerződés részeként kell rögzíteni. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
2.2.2. A 2.2.1. pontban foglalt kötelezettség nem alkalmazandó annyiban, amennyiben az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály határozza meg.
2.2.3. Amennyiben az elnök döntése alapján az Alkotmánybíróság közfeladatának ellátása érdekében közös adatkezelői jogviszony létesítése szükséges, úgy a felek között létrejövő írásbeli megállapodás tartalmazza legalább a GDPR 26. cikke szerinti tartalmi elemeket. A szerződés tartalmának összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
2.2.4. A 2.2.3. pont alapján létrejött közös adatkezelői megállapodás lényegét a kapcsolódó adatkezelési

tájékoztató részeként szükséges az érintett rendelkezésére bocsátani.
2.2.5. Az Alkotmánybírósággal szerződéses jogviszonyba kerülő önálló adatkezelő mint címzett kapcsán a szerződés részeként szükséges rendelkezni a személyes adatok védelme és biztonsága érdekében alkalmazandó intézkedésekről. A szerződés adatkezelést érintő részének összeállítása során ki kell kérni az adatvédelmi tisztviselő véleményét.
2.2.6. A Készenléti Rendőrség a személyvédelmi és létesítménybiztosítási feladatai ellátásának érdekében objektumvédelmi videotechnikai és behatolásjelző eszközöket, berendezéseket működtet az Alkotmánybíróság épületében (a továbbiakban: épület) és az épület előtti közterületet érintően. Az épületében működtetett objektumvédelmi videotechnikai és behatolásjelző eszközök, berendezések tekintetében az adatkezelő a Készenléti Rendőrség.
2.2.7. Az épületben működtetett be- és kiléptető rendszer tekintetében a GDPR 26. cikk (1) bekezdése értelmében az Alkotmánybíróság és a Készenléti Rendőrség közös adatkezelőknek minősülnek.

2.3. Az adatvédelmi tisztviselő kinevezése, jogállása és feladatai

2.3.1. Az adatvédelmi tisztviselő nevét és elérhetőségét az Alkotmánybíróság honlapján közzétett adatkezelési tájékoztatók útján nyilvánosan elérhetővé kell tenni.
2.3.2. Az adatvédelmi tisztviselő halaszthatatlan feladatait, így különösen az adatvédelmi incidensek kezelésével kapcsolatos teendőit távollétében, akadályoztatása, vagy érintettsége esetén a gazdasági főigazgató vagy az általa helyettesítésre eseti jelleggel kijelölt foglalkoztatott (a továbbiakban együtt: helyettes) látja el.
2.3.3. Amennyiben az adatvédelmi tisztviselő helyettese az ellátandó feladata kapcsán – összeférhetetlensége, a minősített adatok kezeléséhez szükséges személyi feltételek hiánya, vagy más ok miatt – nem jogosult eljárni, úgy arról haladéktalanul tájékoztatja az elnököt, aki az ügyben a feltételeknek megfelelő eseti helyettest jelöl ki.
2.3.4. Az elnök biztosítja az adatvédelmi tisztviselő és a helyettese számára a hozzáférést és a megfelelő jogosultságokat a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adatokhoz, valamint a rendelkezésére bocsátja a feladatai ellátásához és szakmai ismeretei naprakészen tartásához szükséges eszközöket és erőforrásokat.
2.3.5. Az Alkotmánybíróság adatvédelmi tisztviselője feladatait más, a munkaköri leírásában meghatározott kötelezettségei mellett, attól függetlenül köteles ellátni, az adatvédelmi tisztviselői tisztségével összefüggő kötelezettségei és feladatai ellátása során nem utasítható, és e tisztségének ellátásával kapcsolatban közvetlenül az elnöknek felel.
2.3.6. Amennyiben az adatvédelmi tisztviselő összeférhetetlenséget állapít meg valamely általa ellátandó feladattal összefüggésben, úgy erről köteles haladéktalanul értesíteni az elnököt, és e feladata kapcsán a jogszerű adatkezelés feltételeinek ellenőrzését az elnök döntése alapján köteles a gazdasági főigazgatónak vagy a helyettesítésre kijelölt foglalkoztatottnak delegálni.
2.3.7. Az adatvédelmi tisztviselő a GDPR 39. cikkében foglalt feladatai mellett
a) vezeti az Alkotmánybíróság adatvédelmi nyilvántartását;
b) ellenőrzi az Alkotmánybíróságnál az adatvédelmi és adatbiztonsági követelmények teljesítésülését, különösen érintettől érkező, az Alkotmánybíróság adatkezelését érintő panasz, vagy adatvédelmi incidens bekövetkezte esetén;
c) közreműködik az adatvédelmi incidens kezelésében, kivizsgálásában, és a vizsgálat
eredménye alapján az adatvédelmi incidenst a GDPR 33. cikke szerint bejelenti a felügyeleti hatóság részére;
d) a személyes adatok kezelését igénylő új tevékenység esetén előzetesen is véleményezi a tervezett adatkezelést;
e) megvizsgálja az Alkotmánybíróság által tervezett vagy módosuló adatkezelések érintettekre gyakorolt kockázatát, szükség esetén adatvédelmi hatásvizsgálatot kezdeményez és közreműködik annak lefolyta-

tásában;
f) adatvédelmi szempontból véleményezi az adatfeldolgozóval, közös adatkezelővel vagy más önálló adatkezelővel kötendő megállapodást;
g) új adatkezeléssel járó tevékenység tervezése vagy valamely adatkezelés körülményeinek változása esetén megvizsgálja, hogy szükséges-e azzal kapcsolatban adatkezelési tájékoztató, új adatvédelmi nyilvántartás bejegyzés, vagy más dokumentáció összeállítása, illetőleg a már létező dokumentum módosítása;
h) kezdeményezi az Alkotmánybíróság munkatársainak az adatvédelemmel, információbiztonsággal, valamint az iratkezeléssel összefüggő képzését, részt vesz az ilyen képzéssel kapcsolatos feladatok ellátásában, kijelölés esetén képzést tart;
i) elősegíti az érintetteket megillető jogok gyakorlását, valamint előkészíti az Alkotmánybírósághoz érkez ,őérintetti joggyakorlásra irányuló beadványokra összeállított válaszok tervezetét.
2.3.8. A Szabályzat hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó bármely kérdésben – a hivatali út betartása nélkül, közvetlenül és szabadon megválasztott kapcsolattartási mód szerint – az adatvédelmi tisztviselőhöz fordulhat.
2.3.8.1. Az érintettek panaszt tehetnek az adatvédelmi tisztviselőnek bármely általuk észlelt, az Alkotmánybíróság működését érintő adatvédelmi probléma miatt, amely panaszt, amennyiben annak kivizsgálásához szükséges minden releváns információ rendelkezésre áll, az adatvédelmi tisztviselő köteles 15 napon belül kivizsgálni, és a vizsgálat eredményéről értesíteni az érintettet.
2.3.8.2. Saját helyzetéből fakadó okokra hivatkozva bármely érintett jogosult kérni, hogy az adatvédelmi tisztviselő ne fedje fel kilétét az elnök, vagy bármely más foglalkoztatottja előtt. Az adatvédelmi tisztviselő a kérésnek köteles eleget tenni, még akkor is, ha ennek hiányában a panaszolt adatvédelmi probléma nem orvosolható, azonban erről köteles tájékoztatni az érintettet.
2.3.9. Az adatvédelmi tisztviselő jogosult
a) tájékoztatást, felvilágosítást kérni minden, e Szabályzat hatálya alá tartozó adatkezelésről;
b) minden, e Szabályzat hatálya alá tartozó adatkezelést vizsgálni és minden olyan helyiségbe belépni, ahol adatkezelés folyik;
c) tanácskozási és véleményezési joggal részt venni minden olyan fórumon, ahol a feladatai ellátásával összefüggő kérdések szerepelnek a napirenden,
d) javaslatot tenni közvetlenül az elnöknek valamely személyes adatok kezelését érintő kérdésben.
2.3.10. Az adatvédelmi tisztviselő az ellenőrzései kapcsán és a 2.3.8. pont szerinti vizsgálatával összefüggésben a fentiek mellett
a) felszólíthatja az adatkezelésben résztvevő foglalkoztatottat a jogszerű állapot helyreállítására;
b) kezdeményezheti az elnöknél a vonatkozó adatvédelmi előírások, valamint a kialakult adatkezelési gyakorlat felülvizsgálatát és átalakítását ,vagy az adatkezelést érint őmás szükséges intézkedések megtételét.

3. A beépített és alapértelmezett adatvédelem elvének érvényesülése az Alkotmánybíróságnál

3.1. Adatkezelés kialakításával összefüggő kötelezettségek

3.1.1. A személyes adatok kezelésével járó új tevékenység megkezdése, vagy a folyamatban lévő adatkezelési tevékenységekkel kapcsolatos módosítások hatálybalépése előtt az SZMSZ alapján a feladat ellátásáért felelős szervezeti egység vezetője kezdeményezi az adatvédelmi tisztviselőnél az adatkezelés jogszerű kialakítása, illetve az elszámoltathatóság elvének történő megfelelés érdekében szükséges és arányos intézkedések meghozatalát.
3.1.2. A megkeresésben az adatkezeléssel járó feladat ellátásáért felelős szervezeti egység vezetője rögzíti a tervezett adatkezelés legfontosabb jellemzőit, úgy mint az adatok kezelésére okot adó körülményt, vagy jogszabályi rendelkezést; a feladat ellátásához szükséges adatköröket és azok tervezett forrását vagy

az adatok biztonsága, valamint az érintettekre nézve azonosított kockázatok csökkentése érdekében tervezett intézkedéseket.
3.1.3. Az adatvédelmi tisztviselő érdemben megvizsgálja a megkeresést, aki szükség esetén az előterjesztő szervezeti egységgel történő konzultáció, az értesítés kiegészítése vagy pontosítására történő felhívást követően – javaslatot tesz az elnöknek
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 esetleges közzétételére
vonatkozóan.
3.1.3.1. Ha a tervezett adatkezelés kapcsán alkalmazandó az Infotv. 5. § (5) bekezdésében meghatározott rendszeres felülvizsgálati kötelezettség – mivel az Alkotmánybíróság közfeladatát megállapító uniós jog, törvény, vagy helyi önkormányzat rendelete az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát nem tartalmazza – a javaslatnak a rendszeres felülvizsgálat lefolytatásának időpontjára és módjára is ki kell, hogy térjen.
3.1.3.2. A 3.1.3. pont szerinti javaslat kapcsán az elnök által hozott döntésről az adatvédelmi tisztviselő tájékoztatja a személyes adatkezeléssel járó feladat ellátásáért felelős önálló szervezeti egység vezetőjét.
3.1.4. Kizárólag akkor hivatkozható az Alkotmánybíróság adatkezelési tevékenysége kapcsán a GDPR 6. cikk (1) bekezdés *e)* pontja szerinti jogalap helyett más, a GDPR 6. cikkében foglalt jogalap, ha az adatkezelési tevékenység nem szükséges az Alkotmánybíróság közfeladatának ellátásához, vagy közhatalmi tevékenységének gyakorlásához.
3.1.5. A 3.1.4. pontban foglaltakon túl is kizárólag akkor képezheti az Alkotmánybíróság adatkezelésének jogalapját a GDPR 6. cikk (1) bekezdés *a)* pontja szerinti érintetti hozzájárulás, ha az adatkezelés vonatkozásában igazolható módon nincs az érintett és az Alkotmánybíróság között egyértelműen egyenlőtlen viszony, továbbá szervezési és technikai intézkedésekkel biztosítható, hogy az érintett hozzájárulását bármikor ugyanolyan könnyen visszavonhassa, ahogy azt megadta.
3.1.6. Személyes adatokat továbbítani kizárólag pontosan meghatározott és jogszerű célból, a konkrét esetben közvetlenül hivatkozható jogalap birtokában lehetséges, és a továbbítandó adatok körét az alkalmazandó jogszabályi követelményeket és az iratkezelésre vonatkozó belső előírásokat is mérlegelve az adatkezelés céljához szükséges körre kell szűkíteni.

3.2. Adatbiztonsági követelmények

3.2.1. Az Alkotmánybíróság a kezelésében lévő adatok, információk és az elektronikus információs rendszerek által nyújtott vagy azon keresztül elérhető szolgáltatások bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszer elemeinek sértetlenségét és rendelkezésre állását személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosítandó, az érintettekre nézve megjelenő kockázatokkal arányos, a technológiai fejlődés szempontjából naprakész, zárt, teljes körű és folytonos adminisztratív, logikai és fizikai védelmi intézkedéseket alkalmaz.
3.2.2. Az alkalmazott védelmi intézkedések naprakészen tartása érdekében az SZMSZ szerinti feladatkörük kapcsán az önálló szervezeti egységek vezetői és az adatvédelmi tisztvisel őírásban javaslatot tehet azok pontosítására vagy fejlesztésére az elnöknek.
3.2.3. Az Alkotmánybíróságnál foglalkoztatottak a náluk lévő, személyes adatnak minősülő adatokat tartalmazó iratokat kötelesek munkaidőn túl – és amelyeket lehetséges munkaidőben is – szekrénybe zárva tartani; az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak időtartama alatt tárolhatók.
3.2.4. Az Alkotmánybíróság feladatellátásával összefüggő személyes adatokat is tartalmazó iratot vagy adathordozót az Alkotmánybíróság épületéből kivinni jogszabály előírása alapján, bíróság vagy hatóság kötelező rendelkezése esetén, vagy a szervezeti egység vezetőjének engedélyével munkaköri feladat el-

látásának céljából lehet. A foglalkoztatott ez esetben is köteles gondoskodni az adatbiztonsági követelmények megvalósulásáról.
3.2.5. Az Alkotmánybíróság közös használatú helyiségeiben és közös használatú eszközei kapcsán – így különösen nyomtatók, másológépek, irattárolók esetében – a személyes adatok célhoz kötött felhasználását, valamint integritását és bizalmas jellegét garantáló további előírásokat az érintett önálló szervezeti egység vezetője jogosult a foglalkoztatottak számára meghatározni.
3.2.6. Az Alkotmánybíróságnál szakmai gyakorlatot teljesítő személy az Alkotmánybíróság kezelésében lévő irathoz kizárólag titoktartási nyilatkozat aláírását, továbbá a kezelt adatok biztonságát garantáló szervezési és műszaki intézkedések kialakítását követően férhet hozzá.
3.2.7. Az iratbetekintés jogának gyakorlására az Alkotmánybíróság eljárásának befejezését követően személyesen, vagy jogi képviselő útján van helye az Alkotmánybíróság Ügyrendjében foglaltaknak megfelelően.
3.2.7.1. Az érintett vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes, vagy védett adatokat adott esetben ki kell takarni vagy más módon felismerhetetlenné tenni). Ugyanígy kell eljárni a másolat, kivonat készítésekor is.
3.2.7.2. A bizonyítási eljárás során keletkezett iratokba történő betekintési jog gyakorlása során – az Alkotmánybíróságról szóló 2011. évi CLI. törvény 57. § (8) bekezdésére tekintettel – érintettnek kell tekinteni az indítványozót és az ellenérdekű felet.
3.2.8. A személyes adatokat tartalmazó iratokat, amelyekre nézve az adatkezelés célja megszűnt haladéktalanul, illetve a mindenkor hatályos irattári tervben előírt megőrzési határidő leteltével meg kell semmisíteni, elektronikus iratok esetében a személyes adatokat törölni kell, a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény szerint levéltárba adandó iratokban foglalt adatok és a jogszabálynál fogva kezelendő személyes adatok kivételével.
3.2.9. Az iratok megsemmisítéséről, az adatok törlésről szükséges biztonsági intézkedések mellett kell gondoskodni. E rendelkezést az Alkotmánybíróság iratkezelési szabályzatának és irattári tervének az ügyiratok selejtezésére és levéltárba adására vonatkozó rendelkezéseivel összhangban kell alkalmazni.

3.3. Az adatkezelési műveletek átláthatóságára vonatkozó követelmények

3.3.1. Az Alkotmánybíróság az adatkezelési tevékenységeire vonatkozóan az adatkezelés érintettje számára világos, könnyen értelmezhető és átlátható módon, az adatkezelés céljai mentén a GDPR 13–14. cikke szerinti tartalommal szükséges az adatkezelési tájékoztatókat állít össze.
3.3.2. Az adatkezelési tájékoztatókban foglaltak tartalmi megfelelőségét, naprakészségét és elérhetőségét az adatvédelmi tisztviselő köteles figyelemmel kísérni.
3.3.3. A kizárólag az Alkotmánybíróság foglalkoztatottjait érintő adatkezelési célok kapcsán összeállított adatkezelési tájékoztatókat az Alkotmánybíróság székhelyén elérhető zárt informatikai rendszerében kell a foglalkoztatottak számára elérhetővé tenni.
3.3.4. A foglalkoztatotti jogviszonyt létesítő személyeket a belépéskor szükséges tájékoztatni az őket érintő adatkezelési tájékoztatók elérhetőségéről.
3.3.5. Az Alkotmánybíróság székhelyén személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről az Alkotmánybíróság beléptető pontjánál elérhető papíralapú adatkezelési tájékoztató, valamint figyelemfelhívó jelzés útján kell tájékoztatni. Emellett szükség esetén, így különösen látássérültek vagy olvasási, szövegértési képességükben korlátozott érintettek esetében szóbeli tájékoztatás nyújtása is kötelező.
3.3.6. A 3.3.3. és 3.3.5. pontban nem szabályozott érintetti kör esetében az Alkotmánybíróság a honlapján, az „Adatkezelési tájékoztatók” cím alatt közzétéve bocsátja az érintettek rendelkezésére a szükséges tájékoztatást.

3.4. Az adatkezelési tevékenységek nyilvántartása

3.4.1. Az Alkotmánybíróság adatvédelmi tisztviselője elektronikusan, kizárólag az Alkotmánybíróság székhelyén elérhető zárt informatikai rendszerben vezeti az Alkotmánybíróság adatkezelési tevékenységeinek nyilvántartását.
3.4.2. Az adatkezelési tevékenységek nyilvántartása az adatkezelési célok mentén, a GDPR 30. cikke által meghatározott tartalommal összeállított nyilvántartás bejegyzésekből áll, amelynek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatókban foglaltakkal. A nyilvántartás aktualizálását, szükséges módosítását az adatvédelmi tisztviselő végzi.

3.5. Az adatvédelmi hatásvizsgálat lefolytatása

3.5.1. Amennyiben egy tervezett adatkezelés kapcsán az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállnak – mivel annak jellege, hatóköre, körülményei és céljai, vagy az alkalmazott technológiai megoldások kapcsán az valószínűsíthetően magas kockázattal jár az érintettre nézve, vagy a tervezett adatkezelés a felügyeleti hatóság által a GDPR 35. cikk (4) bekezdése szerint összeállított jegyzékében szerepel –az adatvédelmi tisztviselő írásban kezdeményezi annak lefolytatását az elnöknél.
3.5.2. Az adatvédelmi hatásvizsgálat lefolytatásának GDPR 35. cikkében foglalt feltételei fennállásának vizsgálata keretében figyelemmel kell lenni arra is, hogy alkalmazható-e valamely, a lefolytatás kötelezettsége alóli kivételszabály, így különösen a kötelező adatkezelést előíró jogszabály kapcsán készült-e adatvédelmi hatásvizsgálat, illetve elérhető-e azonos tárgyban készült adatvédelmi hatásvizsgálat.
3.5.3. Az 3.5.1. szerinti feljegyzés tartalmazza
a) az adatvédelmi hatásvizsgálat lefolytatására okot adó legfontosabb szempontokat;
b) az alkalmazni javasolt módszertan megjelölését;
c) az adatvédelmi hatásvizsgálatba bevonni tervezett szervezeti egységeket és személyeket;
d) a tervezett adatkezelés érintettjei véleményének kikérése kapcsán javasolt megoldást, vagy annak jogszerű mellőzésére okot adó körülményeket;
e) amennyiben az előre megítélhető, a hatásvizsgálat lefolytatásának tervezett időrendjét.
3.5.4. Az elnök kikéri az adatvédelmi tisztviselő álláspontját az adatvédelmi hatásvizsgálat szükségessége kapcsán, majd elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait.
3.5.5. Az adatvédelmi hatásvizsgálatot az elnök által kijelölt foglalkoztatottak (a továbbiakban: munkacsoport) végzik.
3.5.5.1. Az Európai Adatvédelmi Testület által elfogadott – vagy a GDPR alkalmazandóvá válását követően fenntartott –, az adatvédelmi hatásvizsgálatra vonatkozó hatályos iránymutatásban foglalt szempontokat és eljárásrendet a munkacsoport köteles figyelembe venni.
3.5.5.2. A munkacsoport az adatvédelmi hatásvizsgálat lefolytatását követően megállapításairól és javaslatairól összefoglaló jelentést készít az elnöknek. A munkacsoport tevékenysége során keletkezett irat-anyag a jelentés kivételével döntés-előkészítő iratnak minősül.
3.5.5.3. Az adatvédelmi hatásvizsgálatot lefolytató munkacsoport munkáját az adatvédelmi tisztviselő, a gazdasági főigazgató – és amennyiben az adatkezelés elektronikus információs rendszert is érint, az elektronikus információs rendszer biztonságáért felelős személy – segíti. Véleményüket legalább a kockázatelemzés, a tervezett intézkedések és az összefoglaló jelentés kapcsán ki kell kérni.
3.5.6. Az adatvédelmi hatásvizsgálatról készült jelentést és a kapcsolódó véleményeket az elnök részére írásban kell előterjeszteni. A tervezett adatkezelés nem kezdhető meg, amíg az elnök el nem fogadja
a) az adatvédelmi hatásvizsgálat eredményes lezárultáról, és az abban a kockázatok csökkentését szolgáló intézkedések bevezetéséről és az adatkezelés jóváhagyásáról szóló jelentést, vagy
b) az adatvédelmi hatásvizsgálat mellőzésének, vagy megszüntetésének okait tartalmazó jelentést.

3.5.7. Amennyiben jogszabály valamely, az Alkotmánybíróság által tervezett adatkezelés kapcsán a GDPR 36. cikke szerinti előzetes konzultációt írna el ,ővagy az adatvédelmi hatásvizsgálatot lefolytató munkacsoport annak szükségessége mellett dönt, az elnök eseti jelleggel jelöli ki az abban az Alkotmánybíróság nevében eljáró személyeket úgy, hogy a munkacsoportban résztvevő személyek és a tervezett adatkezeléssel érintett önálló szervezeti egység foglalkoztatottjai abban nem járhatnak el.

4. Az adatvédelmi incidensek kezelésével kapcsolatos feladatok

4.1. Amennyiben az Alkotmánybíróság foglalkoztatottja adatvédelmi incidens bekövetkezésének gyanúját észleli, haladéktalanul tájékoztatja arról az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő által kijelölt foglalkoztatott a jelzést követően azonnal tájékozódik az eset lényeges körülményeiről és azt követően haladéktalanul írásban értesíti az adatvédelmi tisztviselőt legalább:
a) az adatvédelmi incidens jellegéről, ideértve különösen az észlelés és bekövetkezés feltételezett időpontjáról, az érintett rendszer vagy irat megjelöléséről;
b) a valószínűsíthetően érintett személyek körétől;
c) a valószínűsíthetően érintett személyes adatok kategóriáról, nagyságrendjéről;
d) az általa javasolt halaszthatatlan intézkedésekről;
e) megítélése szerint az érintettek jogaira és szabadságaira gyakorolt hatásának súlyosságáról,
f) az általa javasolt további intézkedésekről.
4.2. Az adatvédelmi tisztviselő soron kívül gondoskodik az adatvédelmi incidens érintettekre nézve megjelenő hatásainak csökkentését szolgáló intézkedések megtételéről.
4.3. Az adatvédelmi tisztviselő megvizsgálja a 4.1. pont szerinti értesítésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja az Alkotmánybíróság információbiztonságért felelős vezetőjét, a gazdasági főigazgatót vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.
4.4. Abban az esetben, ha az adatvédelmi incidens feltételezhetően az Alkotmánybíróság által üzemeltetett elektronikus információs rendszerek biztonságával összefüggésben következett be, az adatvédelmi tisztviselő az Alkotmánybíróság elektronikus információbiztonságért felelős vezetője felé köteles jelezni a bejelentést. Az Alkotmánybíróság elektronikus információbiztonságért 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.
4.5. Amennyiben az adatvédelmi incidens az Alkotmánybíróság által igénybe vett 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.
4.6. Az adatvédelmi tisztviselő a 4.3. pont szerinti 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 szervezeti egység vezetője 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.
4.7. Az adatvédelmi tisztviselő a GDPR 33. cikk (1) bekezdésében meghatározott bejelentési kötelezettség határidőben történő teljesítésének sérelme nélkül, írásban, sürgős esetben szóban tájékoztatja az elnököt az adatvédelmi incidens kapcsán tett megállapításairól és az érintettre nézve megjelenő valószínűsített kockázatokról, valamint javaslatot állít össze az adatvédelmi incidens kapcsán teendő intézkedésekről.
4.8. A szóban nyújtott tájékoztatást és a kezelésre vonatkozó javaslatokat az adatvédelmi incidens elhárítását követően kell írásba foglalni.
4.9. Amennyiben az elnök 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 GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a felügyeleti hatóság által vezetett nyilvántartásba.
4.10. Amennyiben a 4.3. pont szerinti vizsgálatot az adatvédelmi tisztviselő véleménye szerint
a) nem lehet 72 órán belül teljeskörűen lefolytatni, vagy
b) nem lehet megállapítani egyértelműen a rendelkezésre álló adatok alapján az adatvédelmi incidenssel érintettek körét, az azzal érintett adatkört, vagy az adatvédelmi incidens bekövetkezésének valamennyi más lényeges körülményét, úgy az adatvédelmi tisztviselő a rendelkezésre álló adatok alapján, szakaszos bejelentésre tesz javaslatot az elnök részére. A hiányzó adatok megállapítását követően az adatvédelmi tisztviselő intézkedik a teljes bejelentés benyújtása iránt.
4.11. Amennyiben az elnök az adatvédelmi tisztviselő tájékoztatása alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az esemény egyéb körülményei alapján azt szükségesnek látja, a GDPR 34. cikk (3) bekezdésében felsorolt esetek kivételével elrendeli az érintettek tájékoztatását az adatvédelmi incidens kapcsán.
4.12. Amennyiben az adatvédelmi incidenssel érintett természetes személyek tájékoztatására – különösen az érintettek köre vagy a kapcsolattartási adatok biztonságának sérülése miatt – észszerű módon nincs lehetőség, úgy az adatvédelmi tisztviselő az adatvédelmi incidens főbb jellemzőire vonatkozó értesítés soron kívüli közzétételét kezdeményezi az Alkotmánybíróság honlapján.
4.13. Az adatvédelmi tisztviselő a bekövetkezett adatvédelmi incidensekről a GDPR 33. cikk (5) bekezdése szerint, személyes adatokat nem tartalmazó, az Alkotmánybíróság székhelyén elérhető zárt elektronikus információs rendszerben vezet nyilvántartást, amely tartalmazza legalább
a) az adatvédelmi incidenssel érintett irat vagy nyilvántartás, elektronikus információs
rendszer megjelölését vagy azonosítóját;
b) az incidens észlelésének időpontját és a bekövetkezésének megállapított vagy valószínűsített időpontját;
c) az érintett személyes adatok körét;
d) az incidens hatásait, következményeit, valamint az orvoslásukra tett intézkedéseket;
e) annak ténye, hogy az adatvédelmi incidenst bejelentették a felügyeleti hatóságnak, vagy annak rövid indokolását, ami miatt nem jelentették be.

5. Az érintetti joggyakorlás biztosítására vonatkozó előírások

5.1. Az Alkotmánybíróság – a GDPR 5. cikkében foglalt adatkezelési elvek sérelme nélkül, a GDPR 32. cikke szerinti technikai és szervezési intézkedések végrehajtása mellett – az Alkotmánybíróság adatkezelésére vonatkozó, érintetti joggyakorlásra irányuló minden beadvány kapcsán – a GDPR 13–14. cikk szerinti tájékoztatás kivételével – esetileg és érdemben vizsgálja azt, hogy elsősorban a kérelmet benyújtó természetes személy kilétével, másodsorban az adatkezelés érintettje az Alkotmánybíróság általi azonosításával kapcsolatban merülhetnek-e fel kétségek.
5.1.1. Az Alkotmányíróság az ellenkező bizonyításáig a kérelmet előterjesztő személy megfelelő azonosí-

tásának ismeri el a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 34. §-a szerint megvalósuló beadványokat, a teljes bizonyító erejű magánokiratokban foglalt postai úton előterjesztett és az érintett azonosításához szükséges adatokat tartalmazó kérelmeket, valamint az Alkotmányíróság kezelőirodája munkatárásának a személyazonosság okirattal történő előzetes igazolását követően személyesen átadott beadványokat.

5.1.2. Amennyiben egy érintetti joggyakorlásra irányuló beadvány kapcsán a kérelmet benyújtó természetes személy kilétével kapcsolatban nem merül fel kétség, azonban az Alkotmánybíróság által kezelt adatok körében megállapítást nyer, hogy az érintett nem azonosítható – ,így különösen mert az Alkotmánybíróság adatkezelésének célja nem teszi szükségessé az érintettnek az Alkotmánybíróság általi azonosítását és bizonyítani tudja, nincs abban a helyzetben, hogy azonosítsa az érintettet –erről haladéktalanul írásban tájékoztatja a kérelmet benyújtó személyt.

5.1.3. Abban az esetben, ha a kérelmet előterjesztő személy megfelelő azonosítására nem alkalmas beadvány érkezik az Alkotmánybírósághoz, és abban valamely érintett kapcsolattartási adataira vonatkozó helyesbítéshez való jog gyakorlására irányuló kérelem van, az Alkotmánybíróság hivatalból is köteles vizsgálni, hogy az általa kezelt kapcsolattartási adatok naprakészek-e. A pontosság elvének történő megfelelés érdekében különösen az Alkotmánybíróság által kezelt adatok összevetése lehet indokolt a személyiadat- és lakcímnyilvántartásban nyilvántartott és a Rendelkezési Nyilvántartásban szerepl őadatokkal.

5.2. Az érintetti jogok gyakorlására irányuló kérelem elintézésébe az adatvédelmi tisztviselőt be kell vonni. Az Alkotmánybírósághoz bármely módon – akár nem hivatalos elérhetőségein keresztül, vagy nem megfelelő módon, esetleg formában – előterjesztett, érintetti joggyakorlásra irányuló kérelmet köteles az azt fogadó önálló szervezeti egység vezetője soron kívül az adatvédelmi tisztviselő részére is továbbítani.

5.3. 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 más, iratbetekintési jogát kívánja-e gyakorolni az indítványozó, illetve beadványozó, esetleg közérdekű adatigénylést kíván-e előterjeszteni.

5.4. Az Alkotmánybíróság a hozzáférési jog biztosítása során a harmadik fél jogainak védelmét szem előtt tartva jár el az adatokról készített másolat és az azokba történő betekintés biztosítása során is.

5.5. Az Alkotmánybíróság 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.

5.6. Amennyiben annak a GDPR 12. cikkében foglalt feltételei fennállnak, a válaszadás határideje az elnök döntése szerint további két hónappal meghosszabbítható, azonban ennek megítélése kapcsán részére az 5.5. pont szerinti határidőn belül, írásban kell igazolni a késedelem okait, és előterjeszteni a hosszabbítás kapcsán az érintettnek nyújtandó tájékoztatás tervezetét.

5.7. Az elektronikus úton biztonságosan nem továbbítható személyes adatokat az Alkotmánybíróság postai úton, tértivevényes küldeményben, papír alapú vagy elektronikus adathordozón küldi meg az érintett részére, vagy külön kérésére jegyzőkönyv egyidejű felvétele mellett azt személyesen adja át.

6. Záró rendelkezés

E szabályzat 2026. április 1. napján lép hatályba. Ezzel egyidejűleg hatályát veszti az Alkotmánybíróság Hivatalának XXV-1/2040-0/2016. iktatószámú adatvédelmi és adatbiztonsági szabályzata.

Budapest, 2026. március 18.

Dr. Polt Péter s. k.,
elnök

Alkotmánybírósági ügyszám: XXV/925/2026.

• • •