

MAGYAR NÖVÉNYVÉDŐ MÉRNÖKI ÉS NÖVÉNYORVOSI KAMARA

Belső adatkezelési és adatbiztonsági szabályzat

hatályba lépett 2019. december 12-én

az országos elnökség X/2019.12.12. számú elnökségi határozattal

Jelen Szabályzat **hatálya** kiterjed a Magyar Növényvédő Mérnöki és Növényorvosi Kamara országos és területi szervezeteire, annak valamennyi tisztségviselőjére, szervezeti egységére és az összes foglalkoztatottjára (a továbbiakban Kamara).

A Szabályzat **célja**, hogy biztosítsa a személyes adatok jogszabályban előírt védelmének érvényesülését, az információs önrendelkezés megvalósulását, továbbá, hogy a Kamara által kezelt személyes adatok tekintetében meghatározza az adatkezelés során irányadó adatvédelmi és adatbiztonsági szabályokat.

I. Adatvédelemre vonatkozó rendelkezések

1. Az Adatkezelő törekszik arra, hogy a személyes adatok kezelésének alábbi elvei maradéktalanul érvényesüljenek adatkezelési tevékenysége során:

- a. A Kamara az adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi (jogszerűség, tisztességes eljárás és átláthatóság).
- b. A Kamara a személyes adatok gyűjtését csak meghatározott, egyértelmű és jogszerű célból végzi, és azokat nem kezeli ezekkel a célokkal össze nem egyeztethető módon (célhoz kötöttség).
- c. A Kamara az adatkezelést annak célja(i) szempontjából megfelelően és relevánsan, és a szükségesre korlátozva végzi (adattakarósság). Ennek megfelelően a Kamara nem gyűjt és nem tárol több adatot, mint amennyi az adatkezelés céljának a megvalósulásához feltétlenül szükséges.
- d. A Kamara adatkezelése pontos és naprakész. A Kamara minden észszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek (pontosság).
- e. A Kamara a személyes adatokat olyan formában tárolja, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, figyelemmel a vonatkozó jogszabályokban meghatározott tárolási kötelezettségre (korlátozott tárolhatóság).
- f. A Kamara megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, ideértve a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmét (integritás és bizalmas jelleg).
- g. A Kamara a fentiekben részletezett alapelveknek való megfelelést biztosítja, továbbá a Kamara igazolja ezen megfelelést (elszámoltathatóság). Ennek értelmében a Kamara gondoskodik a jelen belső szabályzatban foglaltak

folyamatos érvényesüléséről, az adatkezelésének folyamatos felülvizsgálatáról, szükség esetén az adatkezelési eljárások módosításáról, kiegészítéséről.

2. A Kamara a Személyes adatok kezeléséről szóló tájékoztatójában (<https://magyarorvos.hu/adatvedelem-gdpr>) meghatározta az érintettek jogait és azok érvényesítésének módját.

3. Az adatkezelési tevékenységek nyilvántartását a Kamara az elszámoltathatóság elvéből következően annak érdekében végzi, hogy az GDPR-nak való megfelelést nyomon tudja követni, és igazolni tudja, így a felelősségébe tartozóan végzett adatkezelési tevékenységekről legalább az alábbi nyilvántartásokat vezeti:

- a. adattovábbítás nyilvántartása;
- b. érintettek jogainak érvényesítése iránti kérelmek és az arra a Kamara által adott válaszok nyilvántartása;
- c. hatósági megkeresések és az arra a Kamara által adott válaszok nyilvántartása;
- d. adatkezelés megszüntetése iránti kérelmek nyilvántartása;
- e. ügyfelek nyilvántartása;
- f. marketing célú megkeresések nyilvántartása;
- g. munkaviszonnal összefüggő személyes adatok kezelésének nyilvántartása;
- h. munkaerő-felvétel nyilvántartása;
- i. adatvédelmi incidensek nyilvántartása.

II. Adatbiztonságra vonatkozó rendelkezések

1. A Kamara a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázatok mértékének megfelelő szintű adatbiztonságot garantálja mind a papír alapú, mind az elektronikus adatok vonatkozásában. Ennek keretében biztosítja az általa kezelt adatok bizalmasságát, sérthetetlenségét és rendelkezésre állását.

2. A Kamara biztosítja a megfelelő szintű adatbiztonsági intézkedések meghatározása érdekében, hogy a Kamara a kezelésében lévő minden egyes adatállományt a védelmi igény szempontjából értékkel, és biztonsági fokozatba sorol. Ennek keretében elemzi:

- a) a kezelt személyes adatok jogosulatlan megismerésével, megváltoztatásával, törlésével, a hardver- és szoftvereszközök megrongálásával járó kockázatot és a várható kárt;
- b) azt, hogy helyreállítható-e a sérült adatállomány, valamint az esetleges helyreállítás ráfordításait, a személyes adatok reprodukálásához szükséges adatforrások rendelkezésre állását, a manuális háttérnyilvántartásból az elveszített adatok pótlásának lehetőségét;
- c) azt, hogy a kezelt személyes adatok jellegére tekintettel indokolt-e megkülönböztetett biztonsági előírásokat alkalmazni;
- d) az adatbiztonságot veszélyeztető más kockázati elemeket.

3. Az adatkezelés biztonsága megvalósítása érdekében a Kamara technikai, szervezési és adminisztratív intézkedéseket alkalmaz együttesen.

4. A Kamara legalább az alábbi technikai intézkedéseket alkalmazza:

- a) a Kamara a jogosulatlan személyek belépésének kiszűrésére alkalmas beléptetési rendszer működtetésével biztosítja, hogy épületébe/irodájába jogosulatlan személyek ne léphessenek be *[ez lehet elektronikus beléptetési rendszer működtetés; vagy egyszerű kulcsos beléptetés, ahol a kulcs csak belépésre jogosultaknak áll rendelkezésre; vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*
- b) a Kamara az általa mind elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy *[irodák, szerver szobák zárása; monitor fóliák alkalmazása; monitorok olyan módon történő elhelyezése, hogy az azon szereplő adatokra kizárólag a jogosultak láthassanak rá; csak a Kamara által auditált adathordozót lehessen a számítógépekhez csatlakoztatni; vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*.

5. A Kamara a szervezési intézkedések keretében biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá *[jogosultsági szintek meghatározása munkakörönként; számítógépes adatbázisokhoz való hozzáférés jogosultsági szinteknek megfelelő beállítása; a belső számítógépes hálózatba való belépés felhasználó névhez és jelszóhoz kötése; vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*.

6. A Kamara legalább az alábbi adminisztratív intézkedéseket alkalmazza:

- a) A Kamara biztosítja, hogy a személyes adatokhoz való esetleges hozzáférés dokumentációkban nyomon követhető legyen *[tevékenység logolás; épületbe/irodába való beengedés naplózása (akár papír alapon); vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*.
- b) a Kamara biztosítja olyan iratkezelési eljárásrend kialakítását, hogy a hozzá tévesen beérkező személyes adatokat tartalmazó iratok a lehető leghamarabb kiszűrésre kerüljenek, és azokat a lehető legszűkebb személyi kör ismerje meg *[amennyiben a postabontó úgy ítéli meg, hogy ilyen adatot tartalmazó irat birtokába jutott, úgy azt kizárólag erre, vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*.

III. Adatvédelmi incidensek kezelése

1. Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

2. Megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

3. Az adatvédelmi incidenst a Kamara indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott,

bejelenti a hatóságnak. Amennyiben a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késelem igazolására szolgáló indokokat is.

4. Amennyiben az adatvédelmi incidens hatóság számára történő bejelentése szükséges, úgy a bejelentésben:

- 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 Kamara által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

5. Az adatvédelmi incidenst nem kell a hatóságnak bejelenteni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek adatvédelemmel és –biztonsággal kapcsolatos jogaira és szabadságaira nézve.

6. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Kamara indokolatlan késelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről az alábbiak szerint:

- a) közli az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- c) ismertetni kell a Kamara által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

- a) a Kamara 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 értelmezhetlenné teszik az adatokat;
- b) a Kamara 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.

8. Amennyiben a Kamara adatfeldolgozót alkalmaz, úgy az adatfeldolgozó szerződésben ki kell kötni, hogy az adatfeldolgozó köteles a nála bekövetkezett adatvédelmi incidenst haladéktalanul bejelenteni a Kamarának.

IV. Adatvédelmi hatásvizsgálat

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a Kamara 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 értékelhetőek

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

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) személyes adatok különleges kategóriái kezelésének esetében,
- c) nyilvános helyek nagymértékű, módszeres megfigyelése,
- d) jogszabály által előírt egyéb esetekben.

A hatásvizsgálat kérdésében a Kamara maga köteles dönteni, de ennek kötelező eseteit a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (www.haih.hu) közzétette a Európai Parlament és a Tanács (eu) 2016/679 rendelete (GDPR rendelet) 35 § (4) és (5) bekezdés alapján. A jelen Szabályzat hatályba lépésének idején alkalmazandó hatásvizsgálati lista itt érhető el: https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

dr. Tarcali Gábor
elnök