

**AZ UKRÁN ORSZÁGOS ÖNKORMÁNYZAT
HIVATALÁNAK
ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZATA**

Preambulum

Az Ukrán Országos Önkormányzat és Hivatala (a továbbiakban: Hivatal) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatbiztonsági szabályzatot alkotja.

Az Ukrán Országos Önkormányzat és Hivatala tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai, eljárásai során biztosítja a személyes adatok védelmét az Európai Parlament és a Tanács, 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 2016/679 számú rendelete (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) szerint.

1. Adatkezelő adatai

Név:	Országos Ukrán Nemzetiségi Önkormányzat és Hivatal
Székhely:	1065, Budapest, Hajós utca 1
E-mail cím:	ukrcentr@t-online.hu
Telefonszám:	+361/461-01-11
Képviselő:	Szabó Jaroslava
Adatvédelmi tisztviselő:	Fotiadisz Szavvasz

Jelen rendelkezéseket az Ukrán Országos Önkormányzat és Hivatala többi szabályzatának előírásaival összhangban kell értelmezni.

Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadók.

2. A szabályzat célja és hatálya

Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja annak biztosítása, hogy az Országos Ukrán Önkormányzat és a Hivatal adatkezelése megfeleljen a GDPR és az Infotv. előírásainak.

Az adatkezelési műveleteket az Országos Ukrán Önkormányzat és a Hivatal úgy tervezi meg és hajtja végre, hogy az érintettek személyes adatainak védelme, valamennyi adatkezelés során biztosított legyen. Megteszi azokat a technikai és szervezési intézkedéseket, és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés, sérülés, az adatok károsodása és véletlen elvesztése, továbbá az esetleges technikai hozzáférhetetlenné válása ellen.

A szabályzattal az Országos Ukrán Önkormányzat és a Hivatal biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

A szabályzat tárgyi hatálya kiterjed az Országos Ukrán Önkormányzat és a Hivatal folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában és az Infotv. (3) § -ban meghatározott személyes adat kezelése megvalósul.

3. Értelmező rendelkezések

Az értelmező rendelkezések tekintetében az Infotv. 3. §-a valamint a GDPR 4. cikke az irányadó.

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy.

Személyes adat: az érintettre vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy egy, vagy több tényező alapján azonosítható.

Különleges adat: a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját

meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajttatja.

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.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel.

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy 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 irányuló műveleteket végeznek.

4. Személyes adatok kezelésére vonatkozó alapelvek érvényesülése

Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelését az Országos Ukrán Önkormányzat és a Hivatal jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi. Az átláthatóság elvének szellemében biztosítja, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint azt világos és egyértelmű nyelvezetrel fogalmazzák meg.

Jogszerűségi feltételek:

- az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (kötelező adatkezelés);
- az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (kötelező adatkezelés),
- az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges.

Célhoz kötöttség elve

A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat az Országos Ukrán Önkormányzat és a Hivatal nem kezeli ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Adattakarékosság elve

Az Országos Ukrán Önkormányzat és a Hivatal az adattakarékosság elve érdekében a személyes adatok közül csak annyi és olyan adatot kezelhet, amelyek az adatkezelés céljai szempontjából megfelelőek és relevánsak, és a szükséges mértékre korlátozódnak.

Pontosság elve

A személyes adatoknak pontosak és szükség esetén naprakészek. Az Országos Ukrán Önkormányzat és a Hivatal minden észszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törölje vagy helyesbítse.

Korlátozott tárolhatóság elve

A személyes adatok tárolása olyan formában történik, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.

„Integritás és bizalmas jelleg” elv

A személyes adatok kezelését az Országos Ukrán Önkormányzat és a Hivatal úgy végzi, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az elszámoltathatóság elve

Az Országos Ukrán Önkormányzat és a Hivatal felelős a személyes adatok kezelésére vonatkozó alapelveknek való megfelelésért, továbbá a megfelelés igazolhatóságáért.

5. Az adatok felhasználása

Az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így az Országos Ukrán Önkormányzat és a Hivatal eljárásai során csak és kizárólag a hatályos jogszabályok rendelkezése i alapján végez adatkezelést.

Az Országos Ukrán Önkormányzat és a Hivatal által kezelt személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelveinek.

Az Országos Ukrán Önkormányzat és a Hivatal személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az

adatok törlésre kerülnek.

Az Országos Ukrán Önkormányzat és a Hivatal személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi felhatalmazás alapján kezel.

Az Országos Ukrán Önkormányzat és a Hivatal az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

Ha a szabályzat hatálya alatt álló személy tudomást szerez arról, hogy az Országos Ukrán Önkormányzat és a Hivatal által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni. Az Országos Ukrán Önkormányzat és a Hivatal megbízásából adatfeldolgozó tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségeket az adatfeldolgozóval kötött megbízási szerződésben érvényesítendő.

6. Az érintettek jogai

- Előzetes tájékoztatáshoz való jog: Az érintett jogosult a kezelt személyes adatai vonatkozásában az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékozódni.
- Hozzáféréshez való jog: Az érintett jogosult személyes adatairól és az azok kezelésével összefüggő információkról tájékoztatást kérni.
- Helyesbítéshez való jog: Az érintett jogosult, hogy a pontatlanul vagy hiányosan rögzített személyes adatai helyesbítését vagy kiegészítését kérje.
- Adatkezelés korlátozásához való jog: Az érintett jogosult a személyes adatai kezelésének korlátozását kérni, ha sérti jogos érdekeit, vagy amennyiben vitatja a Hivatal által kezelt adatai pontosságát, jogszerűségét, szükségességét.
- Törléshez való jog: Az érintett jogosult arra, hogy kérelmére a Hivatal indokolatlan kérelem nélkül törölje a rá vonatkozó személyes adatokat, az Infotv.-ben meghatározott feltételek fennállása esetén. A Hivatal egyes esetekben jogi kötelezettsége áll fenn bizonyos adatok kezelése tekintetében, ezért az adatok törlési kérelme nem teljesíthető különösen a személyes adatok kezelését előíró, a Hivatalnál alkalmazandó jogi kötelezettség teljesítése, illetve közérdekből.

Az érintett által beadott kérelmet, a benyújtásától számított legrövidebb idő alatt – de legfeljebb 25 napon belül – el kell bírálni és a döntésről az érintettet írásban, vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíteni kell. A tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal kell teljesíteni.

Amennyiben az érintett úgy véli, hogy az Országos Ukrán Önkormányzat és a Hivatal az adatkezelése során megsértette a személyes adatok védelméhez való jogát, az irányadó jogszabályok szerinti jogorvoslással élhet a hatáskörrel rendelkező szerveknél, azaz panasszal élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (NAIH) (cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; postai cím: 1530 Budapest, Pf.: 5.; honlap: www.naih.hu; e-mail cím: ugyfelszolgalat@naih.hu; telefonszám: +36-1/391-1400), vagy az illetékes bírósághoz fordulhat.

7. Az Országos Ukrán Önkormányzat és a Hivatal adatvédelmi rendszere

Az UOÖ elnöke és a Hivatal vezetője az Országos Ukrán Önkormányzat és a Hivatal sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

A szabályzatban előírtak betartatásáért az Ukrán Országos Önkormányzatnál az elnök, a Hivatalnál a hivatalvezető a felelős.

Az Országos Ukrán Önkormányzat és a Hivatal gondoskodik arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

Az Ukrán Országos Önkormányzatnál az elnök, a Hivatalnál a hivatalvezető látja el, egy általa kijelölt adatvédelmi tisztviselő útján.

Az adatvédelmi tisztviselőt szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján kell kijelölni. A Hivatal az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi honlapján, valamint bejelenti ezen adatokat a Nemzeti Adatvédelmi és Információszabadság Hatóság részére.

Az Országos Ukrán Önkormányzat és a Hivatal biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint biztosítja számára, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.

Az elnök és a hivatalvezető adatvédelemmel kapcsolatos feladatai:

- felelős az érintettek GDPR-ban és Infotv-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
- felelős az Ukrán Országos Önkormányzat és a Hivatal által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
- felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért
- felügyeli az adatvédelmi tisztviselő tevékenységét
- vizsgálatot rendelhet el.

Az adatvédelmi tisztviselő adatvédelemmel kapcsolatos feladatai:

- segítséget nyújt az érintett jogainak biztosításában;
- jogsult jelen szabályzat betartását ellenőrizni;
- vezeti az adattovábbítási nyilvántartást;
- részt vesz a NAIH által szervezett adatvédelmi tisztviselők konferenciáján;
- figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását;
- közreműködik a NAIH-tól a Hivatalhoz érkezett megkeresések megválaszolásában és a NAIH által kezdeményezett vizsgálat, illetve adatvédelmi hatósági eljárás során;
- általános állásfoglalás megadása céljából megkeresést fogalmaz meg a NAIH felé, amennyiben egy felmerült adatvédelmi kérdés jogértelmezés útján egyértelműen nem válaszolható meg;
- tájékoztatást és szakmai tanácsot ad az Országos Ukrán Önkormányzat és a Hivatal adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban;
- ellenőrzi az adatvédelmi jogszabályoknak, valamint az Országos Ukrán Önkormányzat és a Hivatal belső szabályzatainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomron követi a hatásvizsgálat elvégzését;
- együttműködik a NAIH-val;
- az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint bármely egyéb kérdésben konzultációt folytat a Hatósággal.

Az adatkezelést végző személy feladata:

- a Szabályzatban meghatározott alapelvek betartása, érvényesítése az adatkezelés során, jelen Szabályzatban meghatározott feladatok ellátása
- elősegíteni az adatkezeléssel érintett személyeket abban, hogy az adatkezeléssel érintett jogait gyakorolhassák,
- részvétel a személyes adatok kezelésével érintett személyek tájékoztatásában,
- az adatvédelmi tisztviselő kérésére közreműködni a személyes adatok kezelésével érintett személyek részére nyújtandó információk biztosításában,
- közreműködik az adathordozhatósági jog érvényesítésében, illetve az adattörlésben, ha az érintett személy adattörlési joga érvényesítésre benyújtott kérelme alapján adattörlésnek van helye,
- a hozzá érkezett adatkezelésre irányuló kérelmeket továbbítja az adatvédelmi tisztviselőnek,
- a hozzá érkezett adathelyesbítési kérelemről az adatvédelmi tisztviselő tájékoztatása,

8. Adatbiztonság

Adatbiztonság követelménye:

- Személyes adatokat is tartalmazó iratot kivinni csak az elnök egyetértésével lehet. Ez esetben is gondoskodni kell arról, hogy az ne vesszen el, ne rongálódjon, vagy ne semmisüljön meg, és tartalma illetéktelen személy, vagy szerv tudomására ne jusson.

- Az iratba az ügyintézőn kívül más személy – az ügyfél betekintési jogán és jogszabály kötelező előírásán túl – csak akkor tekinthet be, ha ezt hivatali tevékenységével összefüggő feladatellátás/jogszabály szükségessé teszi. (pl.: ügyészség, rendőrség, kormányhivatal). Az ügyfél, vagy képviselője betekintési jogának gyakorlása során úgy kell eljárni, hogy ez által mások jogai ne sérülhessenek (a más személyre vonatkozó személyes adatok valamilyen módon ki kell iktatni, el kell takarni). Ugyanígy kell eljárni másolat, kivonat készítésekor is.
- Az iratokat munkaidőn túl – és amelyeket lehetséges munkaidőben is – szekrénybe zárva kell tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt tárolhatók.

Valamennyi, adatkezelésben részt vevő személy kötelezettsége, hogy

- gondoskodjon arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyeljen a nyilvántartás biztonságos tárolására;
- tartsa be az adatkezelésre, adatvédelemre és az adatbiztonságra vonatkozó rendelkezéseket;
- haladéktalanul jelezze az informatika rendszer bárminemű meghibásodását, illetve az adatállomány kezelhetőségében bekövetkezett problémát.

Minden munkatárs köteles az elnököt és az adatvédelmi tisztviselőt tájékoztatni minden olyan eseményről, mely esetben őt jogszerűtlen adatkezelésre kérték fel, utasították, illetve a saját rendszerében bármilyen egyéb illetéktelen adathozzáférést, vagy adatkezelést tapasztalt.

9. Adattovábbítás

A személyes adatokat továbbítani, vagy adatszolgáltatást teljesíteni és a különböző adatkezeléseket összekapcsolni csak akkor lehet, amennyiben ahhoz az érintett hozzájárult, vagy törvény azt előírja, vagy megengedi és az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

Amennyiben az adattovábbítást nem lehet jogszerűen teljesíteni vagy az igény elbírálásához szükséges információkat az igénylő nem jelölte meg, az adattovábbítást meg kell tagadni. A megtagadásról – annak indoklásával együtt – írásban kell értesíteni az igénylőt.

10. Adatfeldolgozás

Az Országos Ukrán Önkormányzat és a Hivatal a személyes adatok kezelése során adatfeldolgozót nem vesz igénybe.

11. Adatkezelői nyilvántartás

Az Országos Ukrán Önkormányzat és a Hivatal a kezelésében lévő személyes adatokkal kapcsolatos adatkezeléseiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet, az Info tv-ben előírt tartalommal.

12. Jogellenes adatkezelés következményei

A Nemzeti Adatvédelmi és Információszabadság Hatóság a személyes adatok kezelésével kapcsolatos jogsérelem esetén felszólíthatja az adatkezelőt a jogsérelem orvoslására a szükséges intézkedések megjelölésével.

A felügyeleti hatóság korrekciós hatáskörében eljárva:

- figyelmezteti az adatkezelőt vagy az adatfeldolgozót, hogy egyes tervezett adatkezelési tevékenységei valószínűsíthetően sértik a GDPR rendelkezéseit;
- elmarasztalja az adatkezelőt vagy az adatfeldolgozót, ha adatkezelési tevékenysége megsértette a rendelet rendelkezéseit;
- utasítja az adatkezelőt vagy az adatfeldolgozót, hogy teljesítse az érintettek az a rendelet szerinti jogai gyakorlására vonatkozó kérelmét;
- utasítja az adatkezelőt vagy az adatfeldolgozót, hogy adatkezelési műveleteit –adott esetben meghatározott módon és meghatározott időn belül –hozza összhangba a GDPR rendelkezéseivel;
- utasítja az adatkezelőt, hogy tájékoztassa az érintettet az adatvédelmi incidensről;
- átmenetileg vagy véglegesen korlátozza az adatkezelést, ideértve az adatkezelés megtiltását is;

13. Adatvédelmi incidens

Az adatvédelmi incidens az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

A Szabályzat hatálya alá tartozó személyek, bármely, az adatkezelő által működtetett informatikai rendszer, vagy manuális adatkezelés esetében haladéktalanul, de legkésőbb 24 órán belül kötelesek jelenteni az adatvédelmi tisztviselő felé, ha adatvédelmi incidens történt, vagy annak gyanúja merül fel.

A természetes személyeknek fizikai, vagyoni vagy nem vagyoni károkat okozhat az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában. Többek között: a személyes adataik feletti rendelkezés elvesztését, vagy a jogaik korlátozását, 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 természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Az adatvédelmi tisztviselő a bejelentés megtörténte után haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. Amennyiben az adatvédelmi incidens érinti az informatikai rendszert is, akkor a bejelentést az informatikáért felelős személy részére is meg kell küldeni.

Az adatvédelmi tisztviselő – informatikai rendszert érintő incidens esetén az informatikáért felelős személlyel együttműködve – megvizsgálja a bejelentést és amennyiben szükséges a bejelentőtől további adatokat kér az incidensre vonatkozóan.

A bejelentő köteles megadni az adatvédelmi incidens bekövetkezésének:

- időpontját, helyét,
- egyéb körülményeit,
- az érintett adatok körét,
- az érintett adatok mennyiségét,
- az érintett személyek körét, számát,
- az adatvédelmi incidens várható hatásait,

- a megelőzésre, következményeinek enyhítésére megtett intézkedések felsorolását.

Az adatvédelmi tisztviselő a felderítés során az alábbi kategóriák valamelyikébe sorolja az adatvédelmi incidenst:

- Alacsony szintű adatvédelmi incidens

A személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy jogellenes adatkezelési eset.

Intézkedések: A tudomásszerzéstől számított 2 napon belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre. Rögzíti az incidenst az incidensek nyilvántartásában.

- Közepes szintű adatvédelmi incidens

A személyes adatok csekély körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy jogellenes adatkezelési eset.

Intézkedések: Haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre. Rögzíti az incidenst az incidensek nyilvántartásában és értesíti a felügyeleti hatóságot 72 órán belül.

- Magas szintű adatvédelmi incidens

A személyes adatok széles körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy jogellenes adatkezelési eset, illetve az adatok körétől függetlenül minden olyan eset, amikor valószínűsíthető, hogy az incidensnek az érintettre hátrányos hatása van, vagy biztosra vehető, hogy az incidensnek az érintettre hátrányos hatása van.

Intézkedések: Haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, melyben részt vesz az adatvédelmi tisztviselőn kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és a az elnök. A munkacsoport meghatározza az incidens kezelési módját és felhívja az intézkedésre jogosult személyt az incidens kezelésre, továbbá – amennyiben szükséges – meghatározza az érintettek értesítésének módját és tartalmát. Az adatvédelmi tisztviselő rögzíti az incidenst az incidensek nyilvántartásában és értesíti a felügyeleti hatóságot 72 órán belül.

Amennyiben az adatvédelmi incidens értékelése vizsgálatot igényel, az adatvédelmi tisztviselő a vizsgálat lefolytatásához szükséges munkatársak bevonásával lefolytatja a vizsgálatot. A vizsgálatnak tartalmaznia kell, hogy az adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó, az érintettek tájékoztatása szükséges-e. Amennyiben nem szükséges az érintettek tájékoztatása, ennek indokait is tartalmaznia kell a vizsgálatnak.

A vizsgálat eredményeként az adatvédelmi tisztviselő javaslatot tesz az adatvédelmi incidenssel érintett szervezeti egység vezetőjének az incidenskezeléshez szükséges intézkedések megtételéhez. A vizsgálat eredményéről az adatvédelmi tisztviselő tájékoztatja a jegyzőt.

Az adatvédelmi incidensről az adatvédelmi tisztviselő nyilvántartást vezet, melynek aktualizálásáról gondoskodik.

A nyilvántartás tartalmazza:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az elhárításra megtett intézkedéseket.

Az adatvédelmi tisztviselő az adatvédelmi incidenst a bekövetkezést követően haladéktalanul, de legkésőbb az incidens bekövetkezésétől számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsítve nem jár kockázattal a természetes személy jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az adatvédelmi tisztviselő köteles ennek okát igazolni a Hatóság részére.

A hatósági bejelentés az alábbi adatokat tartalmazza:

- az adatvédelmi incidens bekövetkezésének, valamint a tudomásszerzés időpontját,
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét, elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit,
- a megtett vagy tervezett intézkedéseket.

Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

Amennyiben a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket.

A tájékoztatásnak tartalmaznia kell:

- az adatvédelmi incidens jellegét,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségét,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
- az adatkezelő által az incidens orvoslására tett intézkedéseket vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Nem kell az érintetteket tájékoztatni:

- Ha olyan technikai, szervezési, védelmi intézkedések kerültek végrehajtásra az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára az adatokhoz való hozzáférést, vagy megakadályozzák az adatok értelmezhetőségét.
- Ha az adatvédelmi incidens bekövetkezését követően olyan intézkedések történtek, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.

- Ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé, vagy egyébként jogszabály kizárja.

14. Záró rendelkezések

A Hivatal tagjai kötelesek jelen Szabályzatban foglaltakat megismerni, az adatvédelmi gyakorlat felülvizsgálatáról és szükség esetén a jelen Szabályzat rendelkezéseinek megfelelő eljárások kialakításáról, valamint gondoskodni arról, hogy az adatkezelést végzők megismerjék, előírásait munkavégzésük során alkalmazzák.

Az Ukrán Országos Önkormányzat Közgyűlése az Ukrán Országos Önkormányzat Hivatala Adatvédelmi és Adatbiztonsági Szabályzatát **29/2024 (03.27) UOÖ sz.** határozatával jóváhagyta.

Jelen szabályzat 2024. április 02-napjától hatályos, mellyel egy időben a korábbi Adatvédelmi és Adatbiztonsági szabályzat hatályát veszti


Szabó Jaroslava
elnök




Dr. Neteša Vitalij
hivatalvezető-helyettes

