Adatkezelés Szabályzat
LEO Benchmark munkacsoport
(tervezet)

1. Az Adatkezelési Szabályzat célja

Az **Adatkezelési Szabályzat (**ezentúl **ASZ)** alapvető célja, hogy a munkacsoport folyamatai és az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az ASZ célja továbbá:

- a titokvédelemre vonatkozó intézkedések betartása
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése
- az adatállományok tartalmi és formai épségének megőrzése
- az adatállományok biztonságos mentése
- az adatvédelem és adatbiztonság feltételeinek megteremtése

A szabályzatban meghatározott védelemnek működnie kell a munkacsoport első hivatalos adatszolgáltatásától kezdve az adatok dokumentált megsemmisítésig.

2. Az Adatvédelmi Szabályzat hatálya

2.1. Személyi hatálya

Az ASZ személyi hatálya kiterjed az LEO Benchmark munkacsoportra (ezentúl LEO-BM) és a munkacsoporttal kapcsolatba kerülő személyekre (adat gyűjtők, LEO további tagjainak képviselői).

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül
- kiterjed a munkacsoport által használt informatikai berendezésekre
- kiterjed a folyamatban szereplő összes dokumentációra
- kiterjed az adatok felhasználására vonatkozó utasításokra
- kiterjed az adathordozók tárolására, felhasználására

2.3 Adatok hatálya

- A munkacsoport ülései során keletkezett adatok
- Az adatgyűjtéshez szükséges regisztrációs adatok
- Adatgyűjtéshez létrehozott formanyomtatványok, választási listák, magyarázatok
- Az adatgyűjtés során keletkezett adatok
- Az adatgyűjtésből származtatott adatok, beleértve a megállapításokat
- Fejlesztés során keletkezett dokumentumok

3. Az adatkezelés során használt fontosabb fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon 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 adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, *(Infotv alapján)*

Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik; *(Infotv alapján)*

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik. *(Infotv alapján)*

Adatkezelő*:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja; *(Infotv alapján)*

Adatfeldolgozó:. az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi; *(Infotv alapján)*

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik. *(Infotv alapján)*

Adatbiztonság: az adatkezelő - illetőleg tevékenységi körében az adatfeldolgozó - köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket, továbbá kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Személyes adat:*:* az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés; *(Infotv alapján)*

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, valamint az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat. *(Infotv alapján)*

4. Jogi környezet
4.1. A személyes adatok kezelésének jogi háttere

Az előfizetők személyes adatainak kezelésével kapcsolatos jogszabályai előírásokat Szolgáltató az adatkezelés minden fázisában köteles betartani. Szolgáltató által végzett adatkezelésre elsősorban az alábbi jogszabályokban rögzített rendelkezések az irányadóak:

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv)
- Az elektronikus hírközlésről szóló 2003. évi C. törvény (továbbiakban Eht.) XVII. fejezetében foglalt rendelkezések
- A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény, (a továbbiakban DM. törvény)
- Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény. (a továbbiakban: Eker törvény)

4.2 További szabályozások:

- MSZ ISO/IEC 27001:2006 egyes ajánlásai

5. Az ASZ biztonsági fokozata

A munkacsoport adatai különböző biztonsági fokozatba tartozhatnak:

- Nyilvánosság számra publikált adatok
- Az egyesület által elérhető adatok
- Adatszolgáltatók által elért adatok
- Munkacsoport által elérhető adatok
- Rendszergazda által elérhető adatok

5.1 A biztonsági fokozat és adat körének összefüggése

(A rövidítések magyarázatát a következő szövegrész tartalmazza.)

	munkacsoport	*regisztrációs*	*alapadat*	*gyűjtési adatok*	*származtatott adatok*	*Fejlesztés során*
Nyilvános	**N**	**N**	**I.a**	**I.a**	**I.a**	**N**
Egyesület	**I.b**	**N**	**I.b**	**I.b**	**I.b**	**N**
Adatszolgáltató	**N**	**I.c**	**I.c**	**I.c**	**N**	**N**
Munkacsoport	**I.d**	**I.d**	**I.d**	**I.d**	**I.d**	**I.d**
Rendszergazda	**N**	**Iadm**	**Iadm**	**Iadm**	**Iadm**	**Iadm**

N – nem férhet hozzá

6. Adatkezelési elvek

A fenti táblázatban megadottak alapján a következő elveket/szabályokat jelentik az egyes rövidítések

Ia) - ***Nyilvánosság*** A LEO-BM munkacsoport eredményeit a nyilvánosság is megismerheti. Ezek összegzett adatok, amelyeknek pontos tartalmát és hozzáférési módját (fizető-nem fizető) a munkacsoport a későbbiekben definiálja. Ennek megfelelően hozzáférhetnek az űrlapbizonyos alapadataihoz (az eredmény értelmezése céljából), az összegzett adatokhoz, és a munkacsoport megállapításaihoz, származtatott eredményeihez.

Ib) – ***Egyesület*** Adatkezelési szempontból az egyesület tagjai a munkacsoport tagjaival közel azonos jogosultsággal bírnak, azzal a megszorítással, hogy munkaanyagokat, tervezeteket és nem ellenőrzött anyagokat a munkacsoport nem ad ki, így az egyesület munkacsoporton kívüli tagjai csak a végső verzióhoz juthatnak hozzá. Így az egyesület tagjai megkaphatják a munkacsoport jegyzőkönyveit, elkészült jelentéseit, a BM felmérő űrlaphoz készített alapadatokat, azon összegzett adatokat, amelyek a gyűjtésből elérhetők számukra és minden előbbiekből származtatott adatot. Természetesen nincs hozzáférésük a fejlesztési információkhoz, illetve a gyűjtésnél mindig csak az adott tag által szolgáltatott egyedi adathoz juthatnak.

Ic) - ***Adatszolgáltató*** Adathozzáférési joga kizárólag az ehhez az adatszolgáltatáshoz szükséges regisztrációs alapadatokat foglalja magába.

Id)- ***Munkacsoport tag*** Az adatkezelési joga csaknem teljesen megegyezik az egyesületi tagnál leírtakkal, azzal a bővítéssel, hogy ők minden köztes anyaghoz, levelezéshez, nem ellenőrzött gyűjtött anyaghoz is hozzáférhetnek, illetve ők állítják elő a származtatott adatokat, következtetéseket..

Iadm) -***Adminisztrátor, fejlesztő*** Az adatokat nyilvántartó rendszert kifejlesztő és később üzemeltető személyek minden, a rendszerrel kapcsolatos adathoz hozzáférhetnek feladatuk ellátásával kapcsolatban és annak érdekében. Ezért ezen személyeknek személyükben feddhetetlennek kell lenniük, garantálniuk kell az adatokhoz való hozzáférés fentieknek megfelelő kezelését, és titoktartási nyilatkozatot kell tenniük. A titoktartási nyilatkozatot ezen szabályzat 1. sz. melléklete tartalmazza.

7. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

7.1. Tervezés, előkészítés (munkacsoport munkája) során előforduló veszélyforrások

- jegyzőkönyv és teszt adatok levelezés során történő kikerülése
- IT tervezési adatok, információk kikerülése, amely lehetővé teszi a későbbi behatolást

7.2. A rendszerek megvalósítása során előforduló veszélyforrások

- nem megfelelő kódolás
- a rendszer nem megfelelő beállítása, elsősorban profilok nem helyes meghatározása által jogosulatlan információhoz történő hozzáférés
- biztonsági beállítások kikerülése

7.3. Az adatgyűjtés során előforduló veszélyforrások

- adatformátum-pontatlanság
- mentés elmaradása műszaki és egyéb okokból – adatvesztés, adatbázis sérülése
- adatszolgáltatók gyűjtés vagy rögzítés során történő hibája

7.4. Az adatértékelés során előforduló veszélyforrások

- adatok helyességének nem megfelelő szűrése (speciális karakter, amely megzavarja az összegzést)
- nem csak összegzett adatok kerülnek ki (egy adott kategóriában csak egy szolgáltató van, ebből lehet következtetni az egyedi adatra)
- adatok nem megfelelő összegzése, abból helytelen megállapítások tétele

8. *Az adatvédelem felelőse*

A védelem felelőse a munkacsoport által megbízott személy.
Jelen szabályzatban foglaltak szakszerű végrehajtásáról a munkacsoport vezetőjének kell gondoskodnia.

8.1. Adatvédelmi felelősök feladatai

- az ASZ-t kezeli, naprakészen tartja, a módosításokat átvezeti
- meghatározza a védett adatok körét
- ellátja az adatkezelés és adatfeldolgozás felügyeletét
- ellenőrzi a védelmi előírások betartását
- kialakítja az adatvédelmi tevékenységet segítő nyilvántartási rendszert
- ismerteti az adatvédelmi feladatokat
- ellenőri tevékenységét adminisztrálja
- felelős az informatikai rendszerek üzembiztonságáért, a szerverek adatairól történő biztonsági másolatok készítéséért és karbantartásáért
- gondoskodik a rendszer kritikus részeinek újra-indíthatóságáról, illetve az újraindításhoz szükséges paraméterek reprodukálhatóságáról
- folyamatosan ellenőrzi a védelmi eszközök működését
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működése és biztonsága szempontjából lényeges paraméterek alakulását
- ellenőrzi a rendszer adminisztrációját

8.2. A munkacsoport vezető ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az ASZ előírásainak betartását
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét

9. Az adatgyűjtési feladat és az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

9.1. A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot
- biztonsági mentésekről, háttértárakról a megsérült adatokat visszaállítani
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást

9.2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait
- a tapasztalatokat

9.3. Az adatgyűjtés és feldolgozás folyamatának védelme

9.3.1 Adatgyűjtés védelme

Az adatgyűjtés során várhatóan olyan harmadik személy fog a saját adataival dolgozni, akire a munkacsoportnak csak részben van befolyása. Ezért az adatbekérő űrlapon kell felhívni az adatszolgáltató figyelmét a gyűjtés során szükséges adatvédelemre és annak megfelelő tárolásra. Mivel az adat a szolgáltatóé, így annak védelméről – ebben a munkafázisban - elsősorban neki kell gondoskodnia.

9.3.2. Az adatrögzítés védelme

- Adatállományt rögzíteni csak tesztelt adathordozóra szabad.
- Az adatrögzítő szoftver védelme: Olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is
- hozzáférési lehetőség:
  - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki, milyen szinten férhet hozzá a kezelt adatokhoz , rögzítő csak saját adatihoz férhet hozzá.
  - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti
  - szerverek rendszergazda jelszavát az informatikai vezető kezeli.
- Az adatrögzítés folyamatához kapcsolódó dokumentációk:
    - adatrögzítési utasítások (felhívó levélen)
    - gépkezelési leírások

9.3.3 Adatfeldolgozás védelme

A védelem a szoftverben kialakított eljárásrendek segítségével valósul meg, amelynek részleteit a rendszer kidolgozása során fogja a munkacsoport elfogadni. Szükséges alapelvek az eljárásrend kialakításához:

- egyedi adatok és adatszolgáltatók azonosíthatóságának elkerülése (kivéve rendszergazda)
- statisztikai eljárásrendek és módszertanok alkalmazása statisztikus megbízásával
- a feldolgozói profilok pontos meghatározása és korrekt beállítása
- a feldolgozói jogosultságok megfelelő biztonságának garantálása
- egyedi mentések tiltása (pl. Excel fájlból történő kimentés tiltása – kivéve munkacsoport)
- a feldolgozási folyamat megfelelő dokumentálása, az informatikai rendszerben az egyes lépések naplózása

- az adatfeldolgozás eredményének többszintű (munkacsoport, elnökség) ellenőrzése -különös tekintettel az adatszolgáltatók azonosíthatóságának kizárására-, jóváhagyás.

9.3.4. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (munkacsoportok tagjai, adatrögzítők) feladata. A központi dokumentumot az Egyesület főtitkára tárolja.
A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

9.4. Szoftver és adatbázis védelem

9.4.1. Adatbázis védelem
A WebFM rendszer Oracle adatbázison fut. Az adatbázishoz való hozzáférést a normál Oracle eljárás rendszerint kell kezelni. Ennek tartalma:
- Automatikus mentés eljárás (RMAN) beállítása
- Időközönkénti dump állomány előállítása
- Az adatbázishoz való hozzáférés jelszavainak titkos kezelése
- Tűzfal felállítása az adatbázis szerver védelmére
- Adatbázis log folyamatos vizsgálata
- Az adatbázis struktúra megértéséhez szükséges információk (rendszerterv, dokumentációk) hozzáférésének tiltása illetéktelenek számára

Mivel rendszer a szolgáltatóé, ezért a cég belső rendelkezéseinek kell megfelelni a fenti elveknek.

9.4.2.Feldolgozó szoftver védelem
A BM adatokat feldolgozó szoftver egy úgynevezett WEB2E web alapú keretrendszerben kerül kialakításra. A rendszer többszintű jogosultságokkal rendelkezik, amelynek. legfontosabb elemei:
- egyedi felhasználónév és jelszó
- jelszó érvényesség beállítása
- jelszó minőség vizsgálata
- felhasználók profilhoz való rendelése
- profilokban az egyes adatkörökhöz való hozzáférés összegzett és egyedi beállítása
- profilokban egyes felhasználói felületek (fülek) hozzáférésének beállítása
- profilonkénti felhasználói rutin hozzáférés beállítása
- egyes mezők hozzáférésének tiltása vagy korlátozása
- mezőkre vonatkozó formátum és egyéb biztonsági ellenőrzések
- a program aszinkron működéséből következő adatmentési biztonság
- saját logolási eljárás

További információk a rendszer kézikönyvében, illetve a tervezés során létrejövő dokumentációkban találhatók.

10. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

10.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.
A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.
Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

10.2. Munkaállomások

A felhasználók az adatrögzítés során saját gépeiken jelentkeznek be. Ezért jelen szabályzat erre nem terjedhet ki.

11. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.
A munkafolyamatba épített ellenőrzés során az ASZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

12. Záró rendelkezések

Jelen szabályzatot a munkacsoport hozta saját és projekt működésének biztosítására. A dokumentumot az egyesület elnöksége ellenjegyzi. Dokumentumban változást a munkacsoport tagja kezdeményezhet, és minősített többségnek (2/3) kell elfogadni.
A dokumentum érvénye ameddig a LEO-BM munkacsoport fenntartja a működését, vagy az keletkezett adatok léteznek az egyesület keretében.

aláírások

Mellékletek:

1. sz. melléklet: Titoktartási Nyilatkozat

1. *sz. melléklet*

TITOKTARTÁSI NYILATKOZAT

A LÉTESÍTMÉNYGAZDÁLKODÁSI ÉS ÉPÜLETÜZEMELTETÉSI SZOLGÁLTATÓK ORSZÁGOS SZÖVETSÉGE *(továbbiakban: LEO)* tevékenységgel kapcsolatba kerülő, a LEO-n kívüli személyek számára

Alulírott …….
név

(lakcím: ……

……

anyja neve: ……)

kijelentem,

hogy a …….. tevékenység során tudomásomra jutó, a LEO működésére vonatkozó vagy általa kezelt információkat és adatokat bizalmas jellegének megfelelően kezelem, a tudomásomra jutó üzleti titkot, valamint a személyes adatokat az erre vonatkozó jogszabályok szerint megőrzöm és az abban foglaltak betartására kötelezettséget vállalok.

Kijelentem továbbá, hogy tisztában vagyok az üzleti titok megsértésének büntetőjogi következményeivel. Ezen felelősségem fennáll azt követően is, hogy a fent megnevezett tevékenység bármely ok miatt lezárul.

Budapest, ……

…….
aláírás