Incidenskezelési Protokoll és Bejelentő Lap

TEENDŐK AI INCIDENS ESETÉN

Incidens: a biztonság olyan sérülése, vagy káresemény várható bekövetkezése, amely adatkezeléssel, modell fejlesztése vagy modellek összekapcsolása során a továbbított, tárolt vagy más módon kezelt adatok jogosulatlan felhasználását, illetéktelen személyek számára hozzáférést eredményezi, úgyszintén, ha mesterséges intelligencia rendszer használata során alapvető jogok sérülhetnek, különös tekintettel az input vagy output adatok, modell működési logikájának diszkrimináció mentességére.

FONTOS: A jelen eljárásrend (protokoll) nem vonatozik a más háttérdokumentum hatálya alá tartozó, pl. adatvédelmi, információbiztonsági, belső ellenőrzése vagy compliance (jogi) eljárásokra, nem helyettesíti azokat, így az azokban foglaltaknak is megfelelően kell eljárni.

Teendők:

1) incidensről való tudomásszerzést követően haladéktalanul, legfeljebb 1 órán belül az **Mesterséges Intelligencia Szolgáltató Központ Igazgatóságot** (a továbbiakban: **AISZK**) emailben értesíteni szükséges: Email: adp.incidens@hun-ren.hu

2) A bejelentő haladéktalanul, legkésőbb 1 munkanapon belül megküldi az AISZK-nak az alábbi bejelentő lapot kitöltve. Az AISZK ügyeletese értesíti közvetlen felettesét, valamint a Szolgáltató, a HUN-REN Magyar Kutatási Hálózat) Központi Szervezeti Egységei jogi és megfelelőségi igazgatóját, marketing és kommunikációs igazgatót, informatikai igazgatót és az adatvédelmi tisztviselőt (Data Privacy Officer/DPO). Az értesítést követően a Szolgáltató említett vezetői a Megrendelő főigazgatójával/ügyvezetőjével, és a bejelentést tevő személlyel közösen megbeszélést hívnak össze.

3) Az incidens orvoslására erre a megbeszélésre a bejelentés kivizsgálására, a várható káresemények elhárítására vagy mérséklésére vonatkozó munka-tervezetet készít határidővel és felelősökkel az AISZK ügyeletese, amit a 2) pontban felsorolt személyek jóváhagynak.

4) Az AISZK ügyeletese a 2) pontban foglalt személyekkel, szükség szerint más szakterületekről bevont kollégákkal együtt értékeli az incidenst és döntést készít elő arról, hogy szükséges-e hatóság felé történő bejelentés, vagy más incidenskezelési eljárás megindítása. A hatóság helyszíni szemléje esetén együtt kell működni, a felügyelő hatóság munkatársának megbízó levelét el kell kérni és ellenőrizni, mire van mandátuma a helyszíni szemle során. Ennek hiányában tájékoztatást kell kérni, a helyszíni szemlét végző személy jogosultságaival kapcsolatban

6) Szükséges esetben az AISZK ügyeletese az érintetteket tájékoztatását kezdeményezi. Amennyiben az esemény adatvédelmi incidensnek minősül, az érintettek és az illetékes hatóság tájékoztatásáról az adatvédelmi jogszabályokban meghatározott feltételek és határidők szerint kell gondoskodni.

7) Az incidens megszűnését követően a kivizsgálásról jegyzőkönyvet kell készíteni, amiben minden eljárási lépést és döntést, meghozott intézkedést, megváltoztatandó gyakorlatot rögzíteni kell.

AI INCIDENS BEJELENTŐ LAP

1	Bejelentő neve, elérhetőségei (email, telefon)	[...]
2	Megrendelő (Kutatási Intézmény/Gazdasági Társaság)	[...]
3	Szervezeti egység	[...]
4	Incidens észlelésének időpontja	[...]
5	Incidens rövid leírása	[...]
6	Érintett Platform / AI-eszköz	[...]
7	Érintett Felhasználó(k)	[...]
8	Érintett adatok	[...]
9	Sérültek--e személyes adatok?	[...]
10	Voltak-e az adatbázisban különleges (pl eü) adatok?	[...]
11	Történt-e jogosulatlan hozzáférés?	[...]
12	Történt-e tiltott adatbevitel?	[...]
13	Történt-e AI Output ellenőrzés nélküli felhasználása?	[...]
14	Magas kockázatú AI-használat gyanúja fennáll-e?	[...]
15	Megtett azonnali intézkedések	[...]
16	Szükséges-e további vizsgálat, ha igen melyek ezek?	[...]