Megfelelőség és Biztonság

Jogszabályi háttér

A Filly Care rendszer a pedagógiai szakszolgálatok adatkezelési és nyilvántartási feladatait támogatja. Az érintett adatok köre – gyermekek személyes adatai, pedagógiai és diagnosztikai tartalmak – fokozott védelmet igényel. A rendszer tervezése és fejlesztése során az alábbi jogszabályi és szabályozási keretek figyelembevételével kerültek kialakításra az adatkezelési és biztonsági megoldások:

- **2011. évi CXC. törvény** a nemzeti köznevelésről – meghatározza a pedagógiai szakszolgálatok feladatrendszerét és az adatkezelés kereteit
- **15/2013. (II.26.) EMMI rendelet** a pedagógiai szakszolgálati intézmények működéséről – szabályozza a vizsgálati és dokumentációs folyamatokat
- **20/2012. (VIII. 31.) EMMI rendelet** a nevelési-oktatási intézmények működéséről – az oktatási intézményeket kötelezi, de mivel a szakszolgálat kimenete (szakértői vélemény) közvetlen input az intézményi adminisztrációhoz, a rendszer biztosítja a szükséges strukturált adatmezőket, hatálykezelést és intézményi átadhatósághoz szükséges metaadatokat
- **1997. évi XXXI. törvény** a gyermekek védelméről és a gyámügyi igazgatásról – az érintett gyermekek személyes adatainak védelme
- **GDPR** (EU 2016/679 általános adatvédelmi rendelet) – a személyes adatok kezelésének európai szintű szabályrendszere
- **NAIH állásfoglalások** – a Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlásai az egészségügyi és pedagógiai adatkezeléssel kapcsolatban

Minden új szoftververzió bevezetése előtt **sérülékenységvizsgálat** kerül elvégzésre, amely azonosítja és orvosolja a potenciális biztonsági kockázatokat.

Megjegyzés: A rendszer nem valósít meg KIR-kapcsolatot. A Filly Care rendeltetése a szakértői vélemény generálásának és a 15/2013. (II.26.) EMMI rendelet szerinti dokumentációs folyamatok támogatása, nem az oktatásügyi nyilvántartórendszerrel való közvetlen integráció.

GDPR-megfelelőség

A rendszer tervezésénél a GDPR elvei – adatminimalizálás, célhoz kötöttség, átláthatóság – meghatározó szempontok voltak.

Adatminimalizálás: Csak azok az adatok kerülnek rögzítésre, amelyek a feladat ellátásához szükségesek. A felesleges adatmezők nem kerülnek be az adatbázisba.

Hozzájáruláskezelés és megőrzési szabályok: Az adatmegőrzési határidők a jogszabályi előírásokhoz igazodnak. A rendszer támogatja az adatok automatikus archiválását és szükség esetén az anonimizálást.

Elfelejtéshez való jog: Egy gondviselő kérésére a gyermekre vonatkozó személyes adatok törölhetők vagy anonimizálhatók, a jogszabályban előírt megőrzési kötelezettségek figyelembevételével.

Adathordozhatóság: Az adatok strukturált, géppel olvasható formátumban (JSON) exportálhatók, megkönnyítve az esetleges rendszerváltást vagy az adatok átadását más intézménynek.

Biztonsági funkciók

Hozzáférés-szabályozás

- **Szerepköralapú és attribútum-alapú hozzáférés (RBAC/ABAC)** – minden felhasználó csak a feladatköréhez szükséges adatokat és funkciókat éri el (részletesen: Felhasználó és Jogosultságkezelés fejezet)
- **Kétfaktoros autentikáció** – opcionálisan bekapcsolható, különösen ajánlott az adminisztrátori fiókok esetén
- **Automatikus kijelentkezés** – meghatározott inaktivitási idő után a rendszer automatikusan kiléptet, megakadályozva a felügyelet nélkül hagyott munkamenetek visszaélésszerű felhasználását
- **Jelszó-komplexitási szabályok** – a rendszer megköveteli az erős jelszavak használatát

Kommunikáció biztonsága

- **SSL/TLS titkosítás** – minden adatforgalom titkosított csatornán zajlik, nincs lehetőség a kommunikáció lehallgatására
- **Session kezelés** – a munkamenetek biztonságos, rendszeresen megújított tokenek alapján működnek

Alkalmazásbiztonsági védelmek

- **SQL injection védelem** – a rendszer paraméteres lekérdezéseket alkalmaz, kizárva az adatbázis-manipuláció lehetőségét
- **XSS védelem** – a felhasználói beviteli adatok automatikusan szanítálásra kerülnek, megakadályozva a rosszindulatú kódbefecskendezést
- **CSRF védelem** – minden érzékeny műveletet azonosító token véd az oldalközi kérés-hamisítás ellen

Adattárolás és mentés

- **AES-256 titkosítás** – a személyes és különleges kategóriájú adatok (diagnosztikai, pedagógiai jellegű adatok) titkosítva tárolódnak nyugalmi állapotban
- **Napi rendszerességű biztonsági mentés** – az adatok automatikusan mentésre kerülnek, biztosítva a visszaállíthatóságot rendszerhiba esetén

- **Adatvesztés elleni védelem** – a mentési politika a GDPR és az 1997. évi XXXI. törvény adatmegőrzési követelményeinek megfelelően kerül kialakításra

Audit napló és visszakereshetőség

A rendszer **teljes körű audit trail-t** vezet: minden fontosabb műveletet rögzít, időbélyeggel, a műveletet végző felhasználó azonosítójával és az érintett objektum azonosítójával együtt.

Naplózott események köre:

- Kérelem létrehozása, módosítása, státuszváltozása
- Szakértői vélemény megnyitása, módosítása, lezárása, visszanyitása
- Vizsgálat beosztása, módosítása, eredmény rögzítése
- Felhasználói bejelentkezések és kilépések
- Adminisztratív műveletek (felhasználókezelés, sablonmódosítás)
- Dokumentum generálás és letöltés

Az audit napló **visszakereshetőséget** biztosít: bármely korábbi esemény rekonstruálható, ami különösen fontos jogi vagy vizsgálati helyzetekben. A napló hozzáférése korlátozott – csak az arra jogosult adminisztrátorok és felső vezetők férhetnek hozzá.

Compliance dashboard: az intézményi adminisztrátorok felületen nyomon követhetik a jogszabályi megfelelőségi állapotot. **Hatósági export:** a rendszer lehetővé teszi az adatok exportálását GDPR- és 15/2013. EMMI rendelet szerinti hatósági megkeresések teljesítéséhez. A NIS direktíva figyelembevételével a rendszer szerepének és a kezelt adatok érzékenységének megfelelő biztonsági intézkedések kerülnek alkalmazásra.

20/2012. EMMI rendelet – indirekt megfelelőség

A 20/2012. rendelet az oktatási intézményeket kötelezi arra, hogy a szakértői vélemény alapján egyéni bánásmódot, mentesítést, fejlesztő foglalkozást és értékelési módosítást rendeljenek el. Ha a szakszolgálat dokumentuma nem tartalmazza a szükséges strukturált adatokat, az intézmény nem tud jogszerűen eljárni.

A Filly Care az alábbiak biztosításával teljesíti ezt az indirekt megfelelési kötelezettséget:

- **Kötelező intézményi adatmezők** a szakértői véleményben: ellátás típusa (SNI/BTMN), javasolt fejlesztési óraszám, fejlesztés típusa, felmentési javaslat, értékelési módosítás javaslata
- **Hatálykezelés**: érvényességi dátum, következő felülvizsgálat esedékessége, hatály státusz (aktív/lejárt)
- **Intézményi átadhatóság**: egyedi dokumentumazonosító, verziószám, kiadás dátuma, módosítástörténet

Részletesen: lásd a Szakértői Vélemények fejezet „Intézményi felhasználhatóság és hatálykezelés" alszekciójában.

Szakmai dokumentáció megfelelősége

A rendszer a 15/2013. (II.26.) EMMI rendelet dokumentációs követelményeit az alábbiak szerint teljesíti:

- **Kötelező mezők és dokumentumtípusok** – a kérelmek, vizsgálati dokumentumok és szakértői vélemények esetén a jogszabály által előírt adatmezők kötelezőként vannak konfigurálva; a dokumentum nem menthető, amíg ezek nincsenek kitöltve
- **Verziókövetés** – a szakmai dokumentumok (szakértői vélemények, fejlesztési tervek) minden módosítása verziószámmal és időbélyeggel rögzítésre kerül
- **PDF és XML export** – a dokumentumok PDF formátumban tölthetők le; az adatok XML formátumban is exportálhatók hatósági megkeresések és rendszerközi adatátadás céljából
- **Felülvizsgálati kérelmek és határidők** – a rendszer a felülvizsgálati eljárásokhoz kapcsolódó határidőket nyomon követi és értesítést küld közeledésükkor

WCAG 2.1 AA – Akadálymentesítés

A rendszer felhasználói felülete a **WCAG 2.1 szabvány AA szintjének** figyelembevételével került kialakításra, különös tekintettel a pedagógiai és fejlesztő szakemberek adminisztratív munkakörnyezetére. Mivel a rendszer elsősorban szakértői és vizsgálói felhasználásra készült, teljes körű látássérült-kompatibilitást (screen reader optimalizálás) nem valósít meg, de kiemelt figyelmet fordít a következőkre:

Biztosított akadálymentesítési jellemzők:

- Megfelelő kontrasztarányok (minimum 4.5:1) a szöveg és háttér között
- Billentyűzet-alapú navigáció – egér nélkül is teljesen kezelhető az alkalmazás
- Reszponzív nagyítási lehetőség (minimum 200%) tartalom-veszteség nélkül
- Logikus navigációs struktúra és fókuszkezelés
- Hibaüzenetek egyértelmű, nem kizárólag vizuális megjelenítése

Az akadálymentesítési megoldások elsősorban a pedagógiai és adminisztratív szakemberek munkahatékonyságát szolgálják.