INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

az IDPR-t igénybe vevő
felhasználó szervezetek számára
v1.0

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény) értelmében az Integrált DKÜ Portál Rendszer **központi rendszernek**[1] (a továbbiakban: IDPR vagy központi rendszer, rendszer) **minősül, a rendszert igénybe vevő szervezet felhasználó szervezetnek**[2]. **Az IDPR, mint központi rendszer felett rendelkezési jogot gyakorló szervezet a Digitális Kormányzati Ügynökség Zrt.** (a továbbiakban: DKÜ Zrt.).

A Kiberbiztonsági tv. 8. § (1) bekezdés c) pontja alapján a DKÜ Zrt. a felhasználó szervezet számára a központi rendszer védelme érdekében a felhasználó szervezet által a központi rendszer igénybevétele feltételeként betartandó elektronikus információbiztonsági követelményeket az alábbiak szerint határozza meg:

1) Általános kötelezettségek

A felhasználó szervezet az elektronikus információs rendszereinek a nemzeti kiberbiztonsági hatóság részére történő bejelentése során az IDPR, mint központi rendszer használatát – a központi rendszer azonosítására alkalmas adatok, valamint a központi rendszer felett rendelkezési jogot gyakorló szervezet (DKÜ Zrt.) megjelölésével – bejelenti. A felhasználó szervezet a DKÜ Zrt. által meghatározott elektronikus információbiztonsági követelményeket teljesíti, valamint – amennyiben azzal rendelkezik – rögzíti azokat az információbiztonsági szabályzatában.

2) Szerepek és felelősségek

2.1. A felhasználó szervezet kijelöli azokat a személyeket, akik jogosultak a rendszer használatára, és felelősek a hozzáférések igényléséért, módosításáért és megszüntetéséért.
2.2. A felhasználók felelősek a rendszer rendeltetésszerű használatáért, a rájuk bízott hitelesítő adatok védelméért, valamint az információbiztonsági követelmények betartásáért.
2.3. A DKÜ Zrt. felel a rendszer biztonságos működtetéséért, a központi hozzáférés-kezelésért és a biztonsági események kezelésének koordinálásáért.
2.4. A felhasználó szervezet és a DKÜ Zrt. együttműködik az információbiztonsági kockázatok kezelésében és az incidensek kivizsgálásában.

---

[1] Kiberbiztonsági tv. 4. § 60. pontja: „központi rendszer: egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek”.
[2] Kiberbiztonsági tv. 4. § 29. felhasználó szervezet: „központi rendszert, vagy központi szolgáltatást igénybe vevő szervezet”.

3) Biztonságtudatossági képzés
A felhasználó szervezet gondoskodik arról, hogy a rendszerhez hozzáférő felhasználók alapvető információbiztonsági tudatossággal rendelkezzenek, különös tekintettel az adatok bizalmas kezelésére, a jogosulatlan hozzáférések megelőzésére és az incidensek felismerésére.

4) Csatlakozási, hozzáférési és jogosultságkezelési követelmények
A rendszer kizárólag központilag jóváhagyott, egyedi felhasználói azonosítóval érhető el. A felhasználók kizárólag a munkakörük ellátásához szükséges jogosultságokat kaphatják meg, és kötelesek gondoskodni hitelesítő adataik bizalmas kezeléséről.

5) Fájlkezelés, nyomtatás és adathordozók kezelése
A rendszerből letöltött vagy exportált adatok kezelése során biztosítani kell azok jogosulatlan hozzáféréstől való védelmét. Az adatok nyomtatása és külső adathordozóra mentése csak indokolt esetben, a szervezet belső szabályainak megfelelően történhet.

6) Biztonságos böngésző- és munkakörnyezet beállítások
A rendszer elérése naprakész, gyártó által támogatott böngészőből történhet. A felhasználók kötelesek olyan munkakörnyezetet használni, amely védett a jogosulatlan hozzáféréstől.

7) E-mail és elektronikus kommunikáció biztonsága
A rendszerből származó információk elektronikus továbbítása során biztosítani kell, hogy azok kizárólag jogosult címzettekhez kerüljenek. Bizalmas adatokat tartalmazó információk nyilvános vagy nem védett csatornán történő továbbítása nem megengedett.

8) Adatmegőrzés, archiválás és biztonságos törlés
A rendszerből származó adatok megőrzése kizárólag a jogszabályi vagy működési kötelezettségek által indokolt ideig történhet. Az adatok törlését oly módon kell végrehajtani, hogy azok utólag ne legyenek visszaállíthatók.

9) Hálózatbiztonsági követelmények
A rendszerhez történő hozzáférés során a felhasználó szervezet biztosítja, hogy a hálózati környezet védett legyen a jogosulatlan hozzáférésekkel és ismert támadásokkal szemben.

10) Végpontbiztonság
A rendszerhez hozzáférő végpontoknak (munkaállomás, laptop) rendelkezniük kell alapvető védelmi intézkedésekkel, különösen naprakész operációs rendszerrel és kártékony kód elleni védelemmel.

11) Fizikai biztonsági előírások
A rendszerhez hozzáférő eszközöket olyan környezetben kell használni, amely megakadályozza a jogosulatlan fizikai hozzáférést és az adatok illetéktelen megismerését.

12) Kivételkezelés és kockázatvállalás rendje

A jelen követelményektől való eltérés kizárólag indokolt esetben, dokumentált módon és a kockázatok mérlegelését követően engedélyezhető.

13) Védelmi intézkedések igazolása és dokumentálás

A felhasználó szervezet kérésre igazolja, hogy a jelen dokumentumban meghatározott alapvető információbiztonsági követelményeket alkalmazza.

14) Ellenőrzési jogosultság

A Kiberbiztonsági tv. rendelkezései alapján a DKÜ Zrt. jogosult az IDPR biztonságos használatával összefüggő feladatok végrehajtását indokolt esetben és mértékben a felhasználó szervezeteknél ellenőrizni.

15) Kiberbiztonsági incidensek bejelentése

A felhasználó szervezet az IDPR-t érintő, általa észlelt, Kiberbiztonsági tv. szerinti kiberbiztonsági incidenseket köteles bejelenteni az illetékes kiberbiztonsági incidenskezelő központ és a DKÜ Zrt. részére. A DKÜ Zrt. felé a bejelentéseket az **info@dkuzrt.hu** elérhetőségen tehetik meg.

/Kiberbiztonsági incidensnek minősül az olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát./