EnergyHub Kft.

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

2022. október 11.

Verzió	Jóváhagyta	Dátum	Módosítás oka
3.0	**Tóth Zoltán ügyvezető**	2022.10.11.	

1. Általános rendelkezések

1.1. Jelen adatvédelmi és adatkezelési szabályzat (a továbbiakban: **Szabályzat**) a EnergyHub Kft.-nél (a továbbiakban: **Társaság**) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

1.2. **A szabályzatban foglaltakat kell alkalmazni a konkrét adatkezelési tevékenységek során, valamint az adatkezelést szabályozó vagy azt érintő utasítások és tájékoztatók kiadásakor.**

1.3. Mindenki, aki a Társaság által munkavállalói illetve minden egyéb arra irányuló jogviszony keretében munkajogi kapcsolatba kerül (továbbiakban: Munkatárs) jelen Társasággal, a Szabályzat betartásáért munkajogi, illetve polgári jogi felelősséggel tartozik.

1.4. Jelen szabályzat elkészítése és aktualizálása a Társaság Ügyvezetője, vagy az általa kinevezett felelős vezető feladata.

1.5. A szabályzat felülvizsgálatát évente legalább egyszer és minden jelentős változás esetén el kell végezni.

1.6. A Társaság adatvédelmi tisztviselőt nem alkalmaz.

2. A szabályzat hatálya

Jelen Szabályzat hatálya kiterjed a Társaság tisztségviselőire, munkavállalóira és a Társasággal munkavégzés céljára irányuló egyéb jogviszonyban (megbízási vagy vállalkozási szerződés alapján) foglalkoztatottakra, továbbiakban: Munkatársakra. Az előírásokat az így érintett külsős partnerekre is érvényesíteni kell a szerződéses kapcsolatokban, mely felelőssége és feladatat minden egyes Munkatársnak. .

Jelen Szabályzat visszavonásig érvényes.

3. A szabályzat célja

A Szabályzat kiadásának célja, hogy meghatározza a Társaság és a Munkatársak adatvédelem terén felmerülő feladatait, illetve, hogy a Szabályzat megismerésével és betartásával a Társaság Munkatársai képesek legyenek a természetes személyek adatai kezelését jogszerűen végezni.

A Szabályzat kiadásának további célja, hogy a Társaság tevékenysége során teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, különösen az Európai Parlament és a Tanács (EU) 2016/679 rendeletében foglaltaknak.

4. Lényeges fogalommeghatározások

4.1. **adatkezelő**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;

4.2. **adatkezelés**: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

4.3. **adatfeldolgozó**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

4.4. **személyes adat**: azonosított vagy azonosítható természetes személyre (érintett) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

4.5. **harmadik fél**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, 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 felhatalmazást kaptak;

4.6. **az érintett hozzájárulása**: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a

megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;

4.7. **az adatkezelés korlátozása**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

4.8. **álnevesítés**: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

4.9. **adatvédelmi incidens**: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

4.10. **Munkatárs**: a Társasággal, mint Adatkezelővel munkaviszonyban vagy egyéb, munkavégzésre irányuló jogviszonyban (megbízási, vállalkozási jogviszonyban) levő természetes személy, aki az Adatkezelő szolgáltatásainak ellátásának, teljesítésének feladatával van megbízva, amely tevékenysége során személyes személyes adatokkal kapcsolatba kerül vagy kerülhet, és akinek tevékenységével kapcsolatban az Adatkezelő teljes felelősséget vállal az érintettek személyi köre és harmadik személyek irányában.

5. Az adatkezelés irányelvei

5.1. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

5.2. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet.

5.3. A személyes adatok kezelésének célja megfelelő és releváns legyen, és csak a szükséges mértékű lehet.

5.4. A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni kell.

5.5. A személyes adatok tárolásának olyan formában kell történnie, hogy az érintettek azonosítását csak szükséges ideig tegye lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, ha a tárolás közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.

5.6. A személyes adatok kezelését oly módon kell végezni, 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.

5.7. Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

5.8. A Társaság adatkezelést végző Mukatársa fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozhat a személyes adatok jogszerű kezeléséért. Amennyiben az alkalmazott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

6. Az adatkezelés jogszerűsége

A személyes adatok kezelése akkor jogszerű, ha az alábbiak valamelyike teljesül:

6.1. az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

6.2. 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;

6.3. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

6.4. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

6.5. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

6.6. az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

7. Az adatkezelés felülvizsgálata

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg.

A Társaság Ügyvezetője által megállapított rendszeres felülvizsgálati határidő: 1 év.

8. A Társaság kötelezettségei

8.1. A Társaság a jogszerű adatkezelés érdekében belső adatvédelmi szabályokat alkalmaz, illetve külső és belső adatvédelmi tájékoztatót bocsát ki.

8.2. A Társaság kötelessége, hogy az adatvédelem és adatbiztonság érdekében megfelelő és hatékony intézkedéseket hajtson végre számítástechnikai oldalról is. Ennek keretében biztosítja:

- BIOS védelmét
- BitLocker alkalmazását
- pendrive-ok titkosításának megszervezését
- a tűzfal frissítését
- megfelelő vírusírtó használatát
- GDPR kompatibilis levelező rendszer használatát.

8.3. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre. Ennek keretében:

- A Munkatársak csak a munkájukhoz szükséges mappákhoz rendelkeznek hozzáférési jogosultsággal. A hozzáférési jogosultság szintjét a közvetlen felettes vagy a Társaság Ügyvezetője által kijelölt felelős vezető határozza meg.
- A Társaság területére a beléptetőrendszer segítségével csak az arra jogosultak léphetnek be.
- A papír alapú, személyes adatokat tartalmazó dokumentumok számára zárt szekrény biztosított.

8.3.1. Az adatkezelő vagy az adatfeldolgozó megfelelő nyilvántartást vezet a végzett adatkezelési tevékenységekről.

8.3.2. Az adatvédelmi tudatosság érdekében a munkatársakat oktatja, felkészíti a szabályok alkalmazására.

9. Munkatársak kötelezettségei

9.1. A Munkatárs köteles az adatkezeléssel és adatvédelemmel kapcsolatos szabályokat megismerni és betartani, különös tekintettel a jelen Szabályzat által meghatározott adatbiztonsági követelményekre (ld. 10. pont);

9.2. A Munkatárs csak a feladata ellátásához szükséges mértékben kezelhet adatokat;

9.3. A Munkatárs köteles gondoskodni arról, hogy az adatok ne kerülhessenek illetéktelen harmadik személyek birtokába. Ennek biztosítása érdekében az adathordozó dokumentumokat a közvetlen felügyelete alatt, vagy a munkavégzés helyén, illetéktelenek számára nem hozzáférhető, zárt helyen (lezárt fiókban, szekrényben) kell tartania;

9.4. A Munkatárs köteles gondoskodni arról, hogy az általa használt eszközök felhasználási azonosítójához és jelszavához más, harmadik személy ne férhessen hozzá;

9.5. A Munkatárs adatvédelmi incidens észlelését követően haladéktalanul értesíteni közvetlen vezetőjét;

9.6. A Munkatárs köteles biztosítani, hogy a Társaság tulajdonában illetőleg használatában lévő céges informatikai eszközökön magán jellegű dokumentum vagy fénykép felhasználásra, tárolásra, mentésre ne kerüljön.

10. Adatbiztonsági követelmények és intézkedések

10.1. Általános követelmények

10.1.1. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

10.1.2. Az adatbiztonság megtervezésekor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene a Társaságnak.

10.2. Jelszókezelés

10.2.1. A felhasználói jelszavak generálásának, átadásának bizalmasan kell történnie. A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:

- A Munkatársak kötelesek titkosan kezelni saját jelszavaikat.
- A Munkatársak csak a saját azonosítójukat - szükség esetén a nem a felhasználóhoz rendelt azonosítót – használhatják munkájuk során.
- Egy account első használatakor a Munkatárs köteles megváltoztatni a rendszergazda által a részére átadott/generált jelszót, melyet automatizmussal „kényszerít" ki az adott rendszer.

10.2.2. Amennyiben a felhasználó magára hagyja a számítógépét, kötelessége zárolni az eszközt vagy kijelentkezni a rendszerből.

10.2.3. Amennyiben a Munkatárs személyes jelszava nyilvánossá vált, illetve ennek lehetősége fennáll, úgy köteles azt azonnal megváltoztatni.

10.2.4. Tilos a Munkatársra jellemző, könnyen kitalálható (különösen: vezetéknév, keresztnév, saját gyermekek stb.) jelszavakat választani, a login nevet jelszóként használni, továbbá azonos vagy az abc-ben, a billentyűzeten egymást követő számokból vagy betűkből álló jelszót használni.

10.2.5. A jelszó hossza nem lehet rövidebb nyolc karakternél, tartalmaznia kell legalább egy számjegyet, valamint legalább egy nagybetűt.

10.2.6. Tilos a jelszót nyilvános helyen kiírva tartani (különösen: monitorra ragasztva).

10.3. Mobil informatikai eszközök

10.3.1. A Társaság által rendelkezésre bocsátott mobil számítógépek és mobil telekommunikációs eszközök (pl. okostelefon, tablet) használata során az eszköz védelme érdekében kötelező a PIN kód, ujjlenyomat azonosítás vagy jelszó használata.

10.3.2. A mobil eszközön tárolt munkahelyi adatok biztonságáért az eszköz használója teljes körű felelősséggel tartozik.

10.3.3. A mobil eszközök frissítése kötelező.

10.3.4. Az eszközt számítástechnikai hálózathoz, internethez csatlakoztatni csak biztonságos körülmények szabad. A vezeték nélküli - WiFi, Bluetooth - kapcsolat csak biztonságos körülmények között használható, ezután kikapcsolásuk ajánlott. Nyilvános helyeken elérhető internetes hálózatok használata nem ajánlott.

10.4. Az informatikai rendszerek mentési és archiválási rendje

A Társaság informatikai rendszereiben tárolt adatok és ezen rendszereken futó szolgáltatások megfelelő rendelkezésre állásának érdekében az adatok biztonsági mentési, archiválási és tárolási rendje az alábbiak szerint kialakításra:

10.4.1. Adatok NAS szerverre kerülnek mentésre.

10.4.2. Minden nap biztonsági mentés történik.

10.4.3. Fizikai mentés is történik.

10.4.4. Rendkívüli események által okozott károk enyhítéséért – pl. a hálózati meghibásodások, adatvesztések utáni helyreállítás - a Társaság rendszergazdája a felelős.

10.4.5. A mentések éves rendszerességgel ellenőrzésre kerülnek.

10.5. Adathordozók kezelése

10.5.1. Az adatokat minden külső adathordozón a jelen Szabályzat szerinti biztonsági előírásoknak megfelelően kell tárolni.

10.5.2. Pendrive munkavégzés céljára történő használata esetén kizárólag azon a pendrive használható, amelyet a Digitális Üzletág meghatalmazottja adott ki és informatikailag védett.

10.5.3. Bármely, saját felhasználásba adott, vagy saját tulajdonú, adattárolásra alkalmas informatikai eszköz meghibásodásából adódó adatvesztésért és káreseményért a Munkatárs felel.

10.5.4. Az adathordozó adatainak mentéséért a Munkatárs tartozik felelősséggel.

10.5.5. A Társaság által biztosított adathordozó elvesztése adatvédelmi incidensnek minősülhet, ezért azonnal jelenteni kell a közvetlen felettesnek vagy a Társaság Ügyvezetője által kijelölt felelős vezetőnek.

10.5.6. Amennyiben a Munkatárs káros tartalmat juttat adathordozójával a Társaság informatikai rendszerére, azért személyében felelősséggel tartozik.

10.6. Közösségi oldalak

10.6.1. A Társaság működéséhez kapcsolódó közösségi oldalak adminisztrátori feladatait a Társaság Ügyvezetője által kijelölt felelős személy látja el.

10.6.2. Társaság, a Munkatársak védelmében kifejezetten megtiltja Munkatársak saját vagy társ Munkatársak képeinek, személyes adatainak továbbítását, rögzítését, annak közzé tételét.

10.7. Levelezőrendszer

A Társaság levelezőrendszerének magáncélra történő használata tilos.

Munkatárs mind büntetőjogi, mind polgári peres eljárásban teljes felelősséggel tartozik amennyiben a jelen GDPR szabályokat megszegi

11. Az adatvédelmi incidensek és kezelésük szabályai

11.1. Az adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását.

11.2. Az esetleges adatvédelmi incidenst az Adatkezelő késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

11.3. Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartatása a Társaság ügyvezetőjének, vagy az általa kijelölt felelős vezető feladata.

11.4. Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket, és ezeket folyamatosan elemezni kell.

11.5. A Társaság nyilvántartja az esetleges adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

11.6. Amennyiben a Társaság Munkatársai a feladataik ellátása során adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell közvetlen felettesüket, illetve a Társaság vezetőjét, vagy az általa kijelölt felelős vezetőt.

11.7. Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni, és gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását és a jogszerű működés visszaállítását.

11.8. Az adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

12. A szabályzathoz tartozó egyéb dokumentumok

Jelen Szabályzat elválaszthatatlan részét képezik az 1-5. sz. mellékletek.
Jelen Szabályzattal együtt kell értelmezni és kezelni a Társaság külső és belső adatkezelési tájékoztatóját is.

13. Az adatkezelés alapjául szolgáló jogszabályok

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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 (általános adatvédelmi rendelet vagy GDPR)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2003. évi C. törvény az elektronikus hírközlésről
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény
- a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény
- 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény
- a számvitelről szóló 2000. évi C. törvény