

Budapesti Gépészeti Szakképzési Centrum
Adatvédelmi incidens kockázatbecslése

Adatvédelmi tisztviselő neve: Dr. Hosszú Károly

Adatvédelmi tisztviselő elérhetősége: dr.hosszu@gmail.com

0630/300-4131

I. Hatásvizsgálat és kockázatbecslés

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése, e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. Az adatvédelmi hatásvizsgálatok az elszámoltathatóság szempontjából is jelentőséggel bírnak, ugyanis nemcsak az általános adatvédelmi rendelet (továbbiakban: GDPR) előírásainak teljesítését könnyítik meg az adatkezelők számára, de annak betartása érdekében hozott megfelelő intézkedések végrehajtásának bizonyítását is (lásd: GDPR 5. cikk (2) bekezdés, 24. cikk).

Az adatvédelmi hatásvizsgálat tehát a rendelet betartásának elérésére és bizonyítására szolgáló eljárás.

Adatkezelő az adatvédelmi hatásvizsgálatot a kockázatbecslés eredményétől függetlenül, a folyamatos nyomonkövetés érdekében rendszeresen elkészíti a természetes személyek jogait és szabadságait érintő kockázatok mérséklése érdekében.

II. Kockázatbecslés adatvédelmi incidens esetén

1./ Az adatvédelmi incidens bejelentésének tartalmi elemei

Az új általános adatvédelmi rendelet (továbbiakban: GDPR) 33. cikk (3) bekezdése alapján

A bejelentésben legalább:

- a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket. (Lásd még: Infotv. 25/J.§ (5) bekezdés.)

	személyek, papírok vagy papíralapú továbbítási csatornák)			
Szükségesség és arányosság érvényesülése	- meghatározták a rendelet betartására irányuló intézkedéseket (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekézdés), figyelembe véve az adatkezelés arányosságát és szükségességét előmozdító intézkedéseket (meghatározott, kifejezett és jogos cél(ok) (5. cikk (1) bekezdésének b) pontja); az adatkezelés jogszerűsége (6. cikk); azok megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak (az 5. cikk (1) bekezdésének c) pontja); korlátozott tárolási időtartam (az 5. cikk (1) bekezdésének e) pontja).			
	- meghatározták az érintettek jogait támogató intézkedéseket (az érintetteknek nyújtott tájékoztatás (12., 13. és 14. cikk); betekintési jog és az adathordozhatósághoz való jog (15. és 20. cikk); a			

	helyesbítéshez és a törléshez való jog (16., 17. és 19. cikk); kifogásolási jog és az adatkezelés korlátozásához való jog (18., 19. és 21. cikk); a feldolgozókkal fennálló kapcsolatok (28. cikk); a nemzetközi adattovábbításhoz kapcsolódó garanciák (V. fejezet); előzetes konzultáció (36. cikk))			
Az érintettek jogai és szabadságai	- mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében felmérték a kockázat forrását, jellegét, egyediségét és súlyosságát ((84) preambulumbekzdés) az érintettek szemszögéből			
	- figyelembe vették a kockázatforrásokat ((90) preambulumbekzdés)			
	- beazonosították az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése			

	- beazonosították az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket			
	- felmérték a valószínűséget és a súlyosságot ((90) preambulumbekkezdés)			
Kockázatok kezelését célzó intézkedések bemutatása	- meghatározták a kockázatok kezelését célzó intézkedéseket (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekkezdés), azaz a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat			
	Szakmai egyeztetés: Adatkezelő az adatvédelmi tisztviselő szakmai tanácsát kikérte.			
Adatvédelmi tisztviselő szakmai tanácsa és véleménye	Intézkedési terv			

	véleményezése: Az adatkezelő által a kockázatok mérséklése céljából – az éves adatvédelmi feladatterv - alapján vállalt további intézkedések megfelelőek.			
--	---	--	--	--

V. Kockázati tűréshatár meghatározása

A szervezeti szintű kockázati tűréshatár: Az egész szervezetre - ezen belül szervezeti egységekre és projektekre - vonatkozó összes kockázat mértékét figyelembe véve kerül kialakításra. A vezetés megítéli a kockázatoknak való kitettség elfogadható mértékét és így egy általános tolerancia szintet határoz meg a szervezet számára.

VI. A szervezeti szintű kockázati esemény kockázati értéke, amely az alábbi intézkedéseket igényli (kockázati tűréshatár meghatározása):

Alacsony: A szervezet éves munkatervében, intézkedési tervében megfogalmazott intézkedéseket igényli. Az adatkezelő konzultál a felügyeleti hatósággal.

Közepes: A szervezet éves munkatervében, intézkedési tervében prioritást élvez, a megfogalmazott intézkedések soron kívüli megvalósítását igényli. Az adatkezelő konzultál a felügyeleti hatósággal.

Magas: 30 naptári napon belüli intézkedést igényel. A személyes adatok kezelését illetően az adatkezelő konzultál a felügyeleti hatósággal.

Nagyon magas: Azonnali intézkedést igényel. A személyes adatok kezelését illetően az adatkezelő konzultál a felügyeleti hatósággal.

Az intézkedések célja (megjelölt módszer): A kockázati esemény megszüntetése.

A kockázati kitettség nyomon követése: Az intézkedési terv végrehajtásának év közbeni (évente történő) felülvizsgálata az intézkedésért felelős személy részéről a szervezeten belüli feladatmegosztás szerint.

A kockázatok azonosítására, értékelésére jelen kockázatbecslés eltérő rendelkezésének hiányában a szervezet integrált kockázatkezelésének szabályait kell alkalmazni.

VII. Szervezeten belüli általános feladatmegosztás a hatásvizsgálati/kockázatbecslési (továbbiakban: Hatásvizsgálati) intézkedési terv vonatkozásában

Hatásvizsgálati intézkedési terv	Szervezet vezetője	Folyamatgazda /ák	Munkatársak	Adatvédelmi tisztviselő
Hatásvizsgálati intézkedési terv készítése	Kockázati tűréshatár meghatározása; Jóváhagyás; Munkatársak tájékoztatásának biztosítása az azonosított kockázatokról	Javaslatot tesz a kockázatok csökkentésére vonatkozó stratégiára és a szükséges intézkedések megtételére	Megismeri a szervezet azonosított kockázatait és közreműködik a kockázatok csökkentésére kialakított válaszlépések végrehajtásában	Hatásvizsgálati intézkedési terv véleményezése
Hatásvizsgálati intézkedési terv nyomon követése	Beszámoltatás	Beszámol a Hatásvizsgálati intézkedési terv végrehajtásáról	Visszacsatolást ad a bevezetett intézkedések hatásosságáról	Hatásvizsgálat és a hatásvizsgálati intézkedési terv (adatvédelem éves feladatterv) nyomon követése

Kelt: Budapest, 2021. január 04.



 Varga Csaba kancellár
 Szervezet vezetőjének,
 mint
 Adatkezelő képviselőjének aláírása



.....
 Szervezet adatvédelmi tisztviselőjének aláírása

**Az adatvédelem 2021. évi éves feladatterve, amely tartalmazza a tárgyévi dokumentum iratminták jegyzékét,
valamint a tárgyévi felülvizsgálat (belső audit) rendjét**

Feladat	Határidő	Elérendő eredmény
A munkahelyi adatkezelésről szóló általános adatvédelmi szabályzat és adatvédelmi tisztviselő megbízása (iratminták) összeállítása/ jelen feladatterv alapján elkészített, meglévő dokumentumok felülvizsgálata (továbbiakban: felülvizsgálat)	2021. január 31.	A munkahelyi adatkezelésről szóló általános adatvédelmi szabályzat és adatvédelmi tisztviselő megbízása (iratminták) összeállítása/ jelen feladatterv alapján elkészített, meglévő dokumentumok felülvizsgálata (továbbiakban: felülvizsgálat)
Adatkezelési tevékenység nyilvántartásának és az általános adatvédelmi tájékoztatónak összeállítása/felülvizsgálata (iratminta).	2021. február 28.	Adatkezelési tevékenység nyilvántartásának és az általános adatvédelmi tájékoztatónak összeállítása/felülvizsgálata (iratminta).
Adatfeldolgozásra irányuló megbízási szerződés elkészítése/felülvizsgálata (iratminta).	2021. március 31.	Adatfeldolgozásra irányuló megbízási szerződés elkészítése/felülvizsgálata (iratminta).
Kapcsolattartó hozzájáruló nyilatkozat iratmintájának elkészítése/felülvizsgálata.	2021. április 30.	Kapcsolattartó hozzájáruló nyilatkozat iratmintájának elkészítése/felülvizsgálata.

A szervezet egyes munkáltatói adatkezeléssel kapcsolatos szabályzatának elkészítése/felülvizsgálata.	2021. május 31.	A szervezet egyes munkáltatói adatkezeléssel kapcsolatos szabályzatának elkészítése/felülvizsgálata.
Kockázatbecslés és hatásvizsgálat iratminták elkészítése/felülvizsgálata.	2021. június 30.	Kockázatbecslés és hatásvizsgálat iratminták elkészítése/felülvizsgálata.
Az elektronikus (munkahelyi kamerás) megfigyelőrendszer alkalmazására vonatkozó tájékoztató és érdekmérlegelési teszt iratminta elkészítése/felülvizsgálata.	2021. július 31.	Az elektronikus (munkahelyi kamerás) megfigyelőrendszer alkalmazására vonatkozó tájékoztató és érdekmérlegelési teszt iratminta elkészítése/felülvizsgálata.
A munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnológiai eszköz használatáról szóló megállapodás iratminta elkészítése/felülvizsgálata. A kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló, a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló, valamint az adatvédelmi és adatbiztonsági szabályzat iratminták felülvizsgálata/összeállítása.	2021. augusztus 31.	A munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnológiai eszköz használatáról szóló megállapodás iratminta elkészítése/felülvizsgálata. A kötelezően közzéteendő adatok nyilvánosságra hozatalának rendjéről szóló, a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló, valamint az adatvédelmi és adatbiztonsági szabályzat iratminták felülvizsgálata/összeállítása.

	2021. szeptember 30.	
Az adatvédelmi incidens eljárásrendjének (iratminta) kialakítása/felülvizsgálata. Adatvédelmi incidens kockázatbecslése iratminta összeállítása/felülvizsgálata.	2021. október 31.	Az adatvédelmi incidens eljárásrendjének (iratminta) kialakítása/felülvizsgálata. Adatvédelmi incidens kockázatbecslése iratminta összeállítása/felülvizsgálata.
Az adott évről szóló jelentés/feljegyzés iratminta összeállítása az adatkezelő felé, a következő évre szóló feladatterv összeállítása.	2021. november 30.	Az adott évről szóló jelentés/feljegyzés iratminta összeállítása az adatkezelő felé, a következő évre szóló feladatterv összeállítása.

Megjegyzés:

- Jelen intézkedési terv módosítása esetén a változást követő 5 napon belül az érintett Ügyfelek tájékoztatást kapnak.
- Az adatvédelmi tisztviselő az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság, valamint az informatikai rendszergazda felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele/velük.
- Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.
- Adatvédelmi tisztviselő megbízása nem mentesíti az adatkezelőt jelen feladatterv 1. sz. mellékletét képező adatvédelmi hatásvizsgálat (és kockázatbecslés) teljesítése, valamint a rendszergazda feladatok ellátása/biztosítása és annak költségei alól.

Az elfogadható adatvédelmi hatásvizsgálat szempontrendszere

- módszeres leírás készül az adatfeldolgozásról (a 35. cikk (7) bekezdésének a) pontja):

- ☐ figyelembe vették az adatkezelés jellegét, hatókörét, körülményeit és céljait ((90) preambulumbekezdés);
- ☐ a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítették;
- ☐ funkcionális leírás készült az adatkezelési műveletről;
- ☐ a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) azonosították;
- ☐ figyelembe vették a jóváhagyott magatartási kódexek előírásainak teljesítését (a 35. cikk (8) bekezdése);

- értékelték a szükségességet és az arányosságot (a 35. cikk (7) bekezdésének b) pontja):

- ☐ a rendelet betartására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés), figyelembe véve az alábbiakat:
 - ☐ az adatkezelés arányosságát és szükségességét előmozdító intézkedések a következők alapján:
 - ☐ meghatározott, kifejezett és jogos cél(ok) (az 5. cikk (1) bekezdésének b) pontja);
 - ☐ az adatkezelés jogszerűsége (6. cikk);
 - ☐ megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak (az 5. cikk (1) bekezdésének c) pontja);
 - ☐ korlátozott tárolási időtartam (az 5. cikk (1) bekezdésének e) pontja);
 - ☐ az érintettek jogait támogató intézkedések:
 - ☐ az érintetteknek nyújtott tájékoztatás (12., 13. és 14. cikk);
 - ☐ betekintési jog és az adathordozhatósághoz való jog (15. és 20. cikk);
 - ☐ a helyesbítéshez és a törléshez való jog (16., 17. és 19. cikk);
 - ☐ kifogásolási jog és az adatkezelés korlátozásához való jog (18., 19. és 21. cikk);
 - ☐ a feldolgozókkal fennálló kapcsolatok (28. cikk);
 - ☐ a nemzetközi adattovábbításhoz kapcsolódó garanciák (V. fejezet);
 - ☐ előzetes konzultáció (36. cikk);

- az érintett jogait és szabadságait érintő kockázatokat kezelik (a 35. cikk (7) bekezdésének c) pontja):

- ☐ a kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték ((84) preambulumbekezdés) vagy konkrétabban mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből:
 - ☐ figyelembe vették a kockázatforrásokat ((90) preambulumbekezdés);
 - ☐ az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat beazonosították olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése;
 - ☐ az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket beazonosították;
 - ☐ felmérték a valószínűséget és a súlyosságot ((90) preambulumbekezdés);

☐ az említett kockázatok orvoslására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekkezdés); azaz a kockázatok kezelését célzó intézkedések bemutatása, ideértve a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

- az érdekelteket bevonták:

- ☐ kikérték az adatvédelmi tisztviselő tanácsát (a 35. cikk (2) bekezdése);
- ☐ adott esetben kikérték az érintettek véleményét (a 35. cikk (9))

