

2011/2018/BGSC

Budapesti Gépészeti Szakképzési Centrum

Hatásvizsgálat és kockázatbecslés

Készült: Budapest, 2018. június 05.



I. Hatásvizsgálat

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, kockázati érték meghatározása

	Alacsony kockázati érték	Közepes kockázati érték	Magas kockázati érték	Nagyon magas kockázati érték
Adatfeldolgozás, adatkezelési műveletek	- figyelembe vették az adatkezelés jellegét, hatókörét, körülményeit és céljait ((90) preambulumbekezdés)			
	- rögzítették a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát			

	- funkcionális leírást készítettek az adatkezelési műveletről			
	- azonosították a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, 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) preambulumbekkezdés), 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) preambulumbekzdés)			
Kockázatok kezelését célzó intézkedések bemutatása	- meghatározták a kockázatok kezelését célzó intézkedéseket (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekzdés), 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			

Adatvédelmi tisztviselő szakmai tanácsa és véleménye	Szakmai egyeztetés: Adatkezelő az adatvédelmi tisztviselő szakmai tanácsát kikérte.			
	Intézkedési terv véleményezése: Az adatkezelő által a kockázatok mérséklése céljából – az éves adatvédelmi feladatterv - alapján vállalt további intézkedések megfelelőek.			

III. 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.

IV. 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.

Közepes: A szervezet éves munkatervében, intézkedési tervében prioritást élvez, a megfogalmazott intézkedések soron kívüli megvalósítását igényli.

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

Nagyon magas: Azonnali intézkedést igényel. A személyes adatok kezelését megelőzően 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 hatásvizsgálat eltérő rendelkezésének hiányában a szervezet integrált kockázatkezelésének szabályait kell alkalmazni.

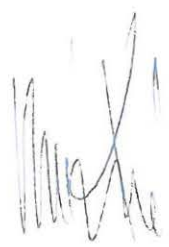
V. Szervezeton belüli általános feladatmegosztás a hatásvizsgálati intézkedési terv vonatkozásában

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:



 Szervezet vezetőjének,
 mint
 Adatkezelő képviselőjének aláírása



 Szervezet adatvédelmi
 tisztviselőjének aláírása

Integritáskontrollnak tekinthetők egyrészt a szervezetre vonatkozó jogszabályok, és az azok alapján készített belső szabályzatok. **Ezek alkotják a kemény kontrollokat.** Másrészt integritáskontrollnak tekintendők a szervezeti értékekkel, elvekkel összefüggésben a **szervezet által készített azon belső szabályozások, amelyeknek megalkotását jogszabály nem írja elő. Ezek az ún. „lágy” kontrollok.** A szervezeti integritás alatt értjük tehát mind a külső szabályozásnak megfelelő, mind a szervezet által kinyilvánított elvek és értékek szerinti működést, azok követését.

* XXX – kritikus kockázat, XX – jelentős kockázat, X – mérsékelt kockázat (Ebben az esetben külön szabályozást nem igényel.)

Szervezet vezetőjének
aláírása