

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 értékkel a kezelésével 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 elkészít a természetes személyek jogait és szabadságait érintő kockázatok mérséklése érdekében. A kockázatbecslés és hatásvizsgálat egységes szerkezetben, az alábbiak szerint történik.

II. Kockázatbecslés és hatásvizsgálat eredménye, kockázati érték meghatározása

| | Alacsony kockázati érték | Közepes kockázati érték | Magas kockázati érték | Nagyon magas kockázati érték |
|------------------------------|---|----------------------------|--------------------------|---------------------------------|
| Adattudományi műveletek | - figyelembe vették az adatkezelés hatókörét, körülmenyeit és céljait (90) preambulumbekedés) | | | |
| Adatteljesítési műveletek | - rögzítették a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát | | | |
| | - funkcionális leírást | | | |

| | | |
|--|--|---|
| | készítettek az adatkezelési műveletet! | |
| | - azonosították a személyes adatokhoz eszközöket (szofiverek, személyek, papíraiapú csatornák) | - meghatározták a rendelet betartására irányuló intézkedéseket (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés), figyelembe véve az adatkezelés arányosságát és szükségességét előmozdító intézkedéseket (meghatározott, kifejezett és jogos cél(ok) (5. cikk (1) bekezdésének b) pontja); az adatkezelés jog szerűsége (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). |
| | | |

| | | | |
|--|---|--|--|
| | <p>- meghatározák az érintettek jogait tárnogató 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))</p> | | |
| | <p>- mindenki kockázat (jogosulttan hozzáférés, nemkívánatos módosítás és az adatok eltüntése) esetében felmérék a kockázat forrását, jellegét, egyediségét és súlyosságát ((84) preambulumbekedés) az érintettek szemszögéből</p> | | |
| | <p>- figyelembe vették a kockázatforrásokat ((90) preambulumbekedés)</p> | | |

| | | | |
|--|--|--|--|
| | <ul style="list-style-type: none"> - beazonosították az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat olyan eseményekre vonatkozóan, mint a jogosulttan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése | | |
| | <ul style="list-style-type: none"> - beazonosították az esetleg jogosulttan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket - felmérték a valószínűséget és a súlyosságot ((90) preambulumbekedés) | | |
| | <ul style="list-style-type: none"> - meghatározták a kockázatok kezelését célzó intézkedéseket (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekedés), azaz a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, intézkedéseket és mechanizmusokat | <p>Kockázatok kezelését célzó intézkedések bemutatása</p> | |

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

III. Kockázati tűréshattár meghatározása

A szervezeti szintű kockázati tűréshatár: Az egész szervezetre - ezen belül szervezeti egységekre és projektekre - vonatkozó összes kockázat mértékét figyelembe véve kerüli kiállításra. 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 munkatermében, intézkedési tervében megfogalmazott intézkedéseket igényli.

Közepes: A szervezet éves munkatermében, 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, értékkelésére jelen hatásvizsgálat elterő rendelkezésének hiányában a szervezet integrált kockázatkezelésének szabályait kell alkalmazni.

V. Szervezeten belüli általános feladatmegosztás a hatásvizsgálati intézkedési terv vonatkozásában

| Hatásvizsgálati intézkedési terv | Szervezet vezetője | Folyamatgazda /ák | Munkatársak | Adatvédelmi tiszttiszelő |
|---|---|--|--|---|
| 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 | Megisméri a szervezet azonosított kockázatait és közreműködik a kockázatok csökkentésére kialakított válaszlepések 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: 2021. 05. 19.



Szervezet vezetőjének,
mint
Adatkezelő-képviselőjének aláírása

.....
Szervezet adatvédelmi tiszttiszelőjének aláírása

1. sz. melléklet

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

| Feladat | Határidő | Elérődő eredmény |
|---|-------------------|---|
| A munkahelyi adatkezelésről szóló általános adatvédelmi szabályzat és adatvédelmi tiszttiselő megbízása (iratminták) összeállítása / jelen feladatterv alapján elkészített, meglévő dokumentumok felülvizsgálata (továbbiakban: felülvizsgálat) | 2021. január 31. | A munkahelyi adatkezelésről szóló általános adatvédelmi szabályzat és adatvédelmi tiszttiselő 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 iratminták elkészítése/felülvizsgálata. | 2021. július 31. | Az elektronikus (munkahelyi kamerás) megfigyelőrendszer alkalmazására vonatkozó tájékoztató és érdekmérlegelési teszt iratminták elkészítése/felülvizsgálata. |
| A munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnológiai eszköz használatáról szóló megállapodás iratminták elkészítése/felülvizsgálata. | 2021. augusztus 31. | A munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnológiai eszköz használatáról szóló megállapodás iratminták elkészítése/felülvizsgálata. |
| A kötelezően közölteendő adatok nyilvánosságra hozatalának rendjéről szóló, a közérdekű adatok megismertésére irányuló igények teljesítésének rendjéről szóló, valamint az adatvédelmi és adatbiztonsági szabályzat iratminták felülvizsgálata / összeállítása. | | A kötelezően közölteendő adatok nyilvánosságra hozatalának rendjéről szóló, a közérdekű adatok megismertésére 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 addott 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 tiszttisztelő az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság, valamint az informatikai rendszergazda felé, valamint addot esetben bármely egyéb kérdésben konzultációt folytat vele/velük.
- Az adatvédelmi tiszttisztelő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülmenyére és céljára is tekintettel végezi.
- Adatvédelmi tiszttisztelő megbízása nem mentesít 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 készüli az adatfeldolgozásról (a 35. cikk (7) bekezdésének a) pontja):

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

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

- a rendelel betartására irányuló intézkedéseket meghatározottak (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulum bekezdés), figyelembe véve az alábbiakat:

- az adatkezelés arányosságát és szükségességet előmozdító intézkedések a következők alapján:
 - meghatározott, kifejezett és jogos cél(ok) (az 5. cikk (1) bekezdésének b) pontja);
 - az adatkezelés jogszervűsége (6. cikk);
 - megfelelők, 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 korlátázásához 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 felmértek ((84) preambulum bekezdés) vagy konkrétabban mindenkor kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből:
 - figyelembe vették a kockázatforrásokat ((90) preambulum bekezdés);
 - 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 eltűnésséhez vezető veszélyeket beazonosították;
 - felmértek a valószínűséget és a súlyosságot ((90) preambulum bekezdés);

az említett kockázatok orvoslására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulum bekezdés);
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:**

- kikértek az adatvédelmi tiszviselő tanácsát (a 35. cikk (2) bekezdése);
- adott esetben kikértek az érintettek véleményét (a 35. cikk (9)