ADATKEZLÉSI- ÉS ADATVÉDELMI SZABÁLYZAT

FEHÉRVÁR MÉDIACENTRUM KFT.

A **FEHÉRVÁR MÉDIACENTRUM KFT.** (továbbiakban: társaság) a munka törvénykönyvéről szóló 2012. évi I. törvény 17. § alapján, továbbá a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 679/2016 rendelet (GDPR) 5. cikk (2) bekezdése alapján az adatkezelés és adatvédelem rendjéről a következő

szabályzatot

alkotja.

Jelen szabályzat hatálya kiterjed a társaság alkalmazottaira és a társaság által kezelt személyes adatokhoz hozzáféréssel rendelkező személyekre.

Jelen szabályzat melléklete tartalmazza a társaság adatkezeléseinek és adatvédelmének szabályait.

Jelen szabályzat a helyben szokásos közzététellel (vezető/szakmai igazgató által tartott értekezlet) válik hatályossá.

Kelt: Székesfehérvár, 2024.augusztus 31.

Hagymásy András ügyvezető

Tartalom

PREAMBULUM

A FEHÉRVÁR MÉDIACENTRUM KFT. (továbbiakban: társaság) tevékenysége során elkötelezett az adatvédelmi és adatbiztonsági előírások betartása iránt. 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 (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: infotv.) mindenkor hatályos szabályain túl a társaság vezetője kiadja jelen adatvédelmi és adatbiztonsági szabályzatot (továbbiakban: szabályzat). A szabályzat az elfogadást követő naptól hatályba lép, és a társaság alkalmazottaival, a társasággal szerződéses kapcsolatban állókkal az őket érintő terjedelemben meg kell ismertetni.

A társaság tevékenységi köréből adódóan tömegtájékoztatási, reklám tevékenységet végez. A társaság a szabályzat elfogadása idején munkavállalókat foglalkoztat így a kapcsolódó adatkezelésekről is jelen szabályzat rendelkezik. A társaság papír alapú adatkezeléseken, nyilvántartásokon túl, elektronikus formában is kezel és tart nyilván adatokat, az adatbiztonsági követelményeket jelen szabályzat szerint teljesíti.

A társaság vállalatirányítási rendszert, számlázó programot, gépjármű-nyomonkövető alkalmazást, webtárhelyet vesz igénybe. A szoftver fejlesztői kötelesek jelen szabályzatban foglaltaknak megfelelő minimális védelmi, jogosultsági szinteket biztosítani és azt igazolni a társaság részére.

A társaság biztosítja informatikai eszközei, hálózatának üzemeltetését (szerverépítés, szoftvertelepítés, konfigurálás, hibaelhárítás, biztonsági ellenőrzés). A társaság gondoskodik megfelelő vírusvédelemről, tűzfalról, biztonsági mentésekről, szünetmentes működésről. Az informatikai eszközöket jelszavas védelemmel látja el, a társaság törekszik a hordozható informatikai eszközök és az elektronikus kommunikáció titkosítására.

A társaság ügyfeleit, munkatársait, illetve a vele bármilyen jogviszonyban álló személyeket nem kategorizálja, nem minősíti, ilyen célból adatot nem kezel.

Az adatvédelmi elveknek a GDPR 25. cikk alapján a társaság valamennyi tevékenysége, döntése során érvényesülnie kell, a társaság törekszik arra, hogy a lehetőségekhez képest olyan adatvédelmi informatikai megoldást, szervezeti szabályozást alkalmazzon, amely az adatok védelmét a tudomány és technika állása szerint a leghatékonyabban biztosítja.

A társaság valamennyi adatvédelmi folyamatának szabályozottnak, átláthatónak, nyomon követhetőnek, konkrét munkakörhöz rendelhetőnek kell lennie.

A társaság törekszik arra, hogy amennyiben meghatározott cél elérése személyes adat kezelése nélkül is elérhető, úgy ne kezeljen személyes adatot.

A társaság a munkavállalói tevékenységét úgy szervezi meg, hogy lehetőleg minél kevesebb munkavállaló kezeljen személyes adatokat, a személyes adatot kezelő munkavállaló pedig a személyes adatok egy csoportját kezelje (pl. személyügyi adatok, kifizetéshez kapcsolódó adatok, ügyfélkapcsolati adatok).

I. RÉSZ

Általános rendelkezések

1. A szabályozás célja, hatálya

1. A társaság adatvédelmi, adatbiztonsági szabályzata (a továbbiakban: Szabályzat) kibocsátásának célja, hogy tevékenysége során a személyes adatok védelméhez fűződő adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározásra kerüljenek az adatvédelmi és adatbiztonsági előírások, továbbá az érintettek jogai megfelelően biztosítva legyenek.

2. A szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy a társaság adatkezelő és adatfeldolgozó tevékenysége megfeleljen 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, a továbbiakban: GDPR) szóló az Európai Parlament és a Tanács 2016/679 rendeletének – (2016. április 27.) – továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) rendelkezéseinek.

3. Jelen szabályzatban nem szereplő kérdésekben a GDPR és az Infotv. szabályai szerint kell eljárni.

4. A Szabályzat hatálya természetes személyre vonatkozó személyes adatok Társaság általi kezelésére terjed ki, egyéni vállalkozó, egyéni cég, őstermelő ügyfeleket, vevőket, szállítókat e szabályzat alkalmazásában természetes személynek kell tekinteni.

5. A Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre – nevükre, formájukra, elérhetőségükre – vonatkozik.

6. **A Szabályzat személyi hatálya** kiterjed:

a) az Adatkezelő valamennyi munkavállalójára.
b) az eseti jelleggel munkavégzésre igénybe vett dolgozóra,
c) az adatfeldolgozóra, valamint
d) a fentieken kívül mindazon személyre, aki az Adatkezelővel bármilyen szerződéses jogviszonyban áll

7. **A Szabályzat tárgyi hatálya** kiterjed:

a) az Adatkezelőnél keletkezett valamennyi személyes és egyéb védendő adatra,
b) az informatikai rendszerben kezelt vagy feldolgozott személyes és egyéb védendő adatra,
c) az adatkezelés eredményeképpen létrejött személyes és egyéb védendő adatra,
d) az Adatkezelőnél alkalmazott valamennyi személyes és egyéb védendő adatot kezelő hardver- és szoftvereszközre,
e) Az Adatkezelő tevékenységével kapcsolatos, működése során keletkező közérdekű adatra vagy közérdekből nyilvános adatra.

8. **A Szabályzat időbeli hatálya**

a) a Szabályzat az alkalmazottakkal való közléstől, visszavonásáig hatályos.
b) Jelen szabályzat kötelezően felülvizsgálandó:

- jelentős szervezeti, vagy jogszabályi változásokat követően,

- a hatályossá válását követő minden harmadik évben, így az első kötelező felülvizsgálat időpontja: 2027.;

- az adatkezelések változása, új adatkezelés bevezetése esetén haladéktalanul.

2. Értelmező rendelkezések

9. **Jelen szabályzat alkalmazása során a GDPR 4. cikkben meghatározott fogalmakat kell érteni, a következő kiegészítésekkel:**

10. **adatbiztonság:** az adatvédelmi incidenst bekövetkezését megelőzni képes szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben a kockázati tényezőket – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.

11. **adatkezelési nyilvántartás:** a GDPR 30. cikke alapján vezetett, személyesadat-kezeléseket tartalmazó nyilvántartás, amely az érintett adatkezeléshez kapcsolódó minden lényeges információt tartalmaz, a dokumentum a **GDPR által előírt kötelező nyilvántartások** mappában található.

12. **adatvédelmi incidens nyilvántartás:** a GDPR 33. cikk (5) bekezdése alapján vezetett nyilvántartás, amely jelen szabályzat a dokumentum a **GDPR által előírt kötelező nyilvántartások** mappában található.

13. **dolgozói személyes adat**: a társasággal munkaviszonyban, egyszerűsített foglalkoztatotti jogviszonyban álló személyek célhoz kötöttség elvének betartásával kezelt adata.

14. **nyilvántartási célú személyesadat-kezelés**: előre meghatározott szempontok alapján gyűjtött személyesadat-fajtákból adott szempontok szerint strukturált papíralapú vagy elektronikus adatállomány, amelyben az adatkezelés időtartama alatt biztosított az adatok különböző jellemzők alapján történő visszakereshetősége, lekérdezhetősége. Nyilvántartási célú adatkezelésnek minősül az is, amennyiben az adatok a nyilvántartás felvételét megelőző ügyfélkapcsolati adatkezelésből származnak, de az adatok kezelése az adatkezelési cél tekintetében elválik az alapeljárástól. Nyilvántartási célú adatkezelésnek is meg kell felelni a GDPR alapelveinek, rendelkezéseinek.

15. **adatállomány***:* az Adatkezelőn belül több nyilvántartó rendszerben kezelt személyes és egyéb védendő adatok összessége.

16. **Egyéb védendő adat**: az üzleti titok védelméről szóló 2018. évi LIV. törvény szerinti Adatkezelő gazdasági tevékenységéhez kapcsolódó üzleti titok és védett ismeret.

II. RÉSZ

Adatvédelem felelősségi rendszere

3. Az adatkezelések szintjei

17. A társaság kapcsolatban áll adatfeldolgozókkal, amelyek kiválasztása körében törekszik a lehető legmagasabb szintű adatvédelmi és adatbiztonsági megoldásokat nyújtó partnerek kiválasztására, ebből a célból előzetesen megismeri az adatfeldolgozók adatvédelmi és adatbiztonsági szabályzatát, illetve az adatfeldolgozói szerződésben rögzítik a vonatkozó szervezeti és informatikai biztonságra vonatkozó rendelkezéseket.

18. A társaság ügyel arra, hogy az adatfeldolgozók lehetőség szerint ne kerüljenek kapcsolatba a munkavállalók, megbízók személyes adataival, amennyiben ez nem kerülhető el, úgy azok – elektronikus, vagy papír alapú – átadása megfelelő biztonsági intézkedések keretében történhet.

4. Az adatkezelő szerv vezetője felelősségi rendszere

19. Az adatvédelemre vonatkozó előírások alkalmazása során adatkezelő szerv vezetőjének kell tekinteni a társaság ügyvezetőjét.

20. Az adatkezelő szerv vezetője felelős:

a) a társaság adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, ennek keretében a szerv által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtételéért;
b) a munkavállalók adatvédelmi oktatásáért és továbbképzéséért;
c) a vezetése vagy irányítása alá tartozó társaság tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) az érintettek jogainak gyakorolásához szükséges feltételek biztosításáért.
e) adatvédelmi tisztviselő kiválasztásáról, alkalmazásáról, vagy megbízásáról.

21. Az adatkezelő szerv vezetőjének felelőssége nem zárja ki a társasággal kapcsolatban álló személyek akár kártérítési, akár büntetőjogi felelősségét.

22. Amennyiben a személyes adatokhoz való jog megsértése miatt a társaságnak sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a személyes adatokhoz fűződő jogsértést ténylegesen elkövető személy kilétének felderítésére mindent meg kell tenni, és amennyiben ez sikerrel jár, vele szemben kártérítési eljárást kell kezdeményezni.

5. Az adatkezelő szerv vezetőjének feladat- és hatásköre

23. Adatkezelő szerv vezetőjének feladat- és hatásköre:

a) a feladat- és hatáskörbe utalt adatkezelési rendszerek egészének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakítása és irányítása, rendeltetésszerű működtetése, melynek keretében teljes felelősséget visel a személyes adatok kezelésére vonatkozó törvények és az ezen alapuló rendelkezések érvényre juttatásáért.
b) gondoskodik a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás, vagy törlés megelőzéséről, a technikai védelemről, továbbá, hogy a személyes adatok védelmének biztosítása érdekében az érintett az adatkezelő által kezelt adataihoz – ha törvény kivételt nem tesz – hozzáférhessen, illetve gyakorolhassa az őt megillető jogokat.
c) személyes felelősséggel tartozik a társaság és az általa alkalmazott, vele szerződéses kapcsolatban állók tevékenységéért, a törvényes és szakszerű működéséért, ezen belül az állomány adatkezelői tevékenységéért, az adatvédelmi előírások, valamint a kapcsolódó ügyviteli szabályok betartásáért.
d) a védelmi és biztonsági szabályok gyakorlati érvényesülésének ellenőrzése, intézkedés a hiányosságok felszámolására;
e) az adatkezelések szervezeti és működési feltételeinek kialakítása, gondoskodás a működési követelmények és az adatbiztonsági követelmények érvényre juttatásáról;
f) az adatkezelések szabályozottságának, dokumentáltságának kialakításáért, ellenőrzéséért;
g) az adatvédelmi kockázatok elemzéséről, hatásvizsgálat lefolytatásáért.
h) gondoskodik az adatkezelések nyilvántartás, az adatvédelmi incidensek nyilvántartás vezetéséről, naprakészen tartásáról.

6. A társaság adatvédelmi tisztviselője

24. A társaság az adatvédelmi szabályoknak való megfelelés érdekében adatvédelmi tisztviselőt bíz meg. A társaság adatvédelmi tisztviselője, amennyiben nem áll alkalmazásában, úgy olyan szerződéssel megbízott vállalkozó, aki szakmai szempontból rátermett, az adatvédelmi jogot és gyakorlatot szakértői szinten ismeri, a feladatok ellátására alkalmas.

25. A társaság az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el, szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül a társaság ügyvezetőjének tartozik felelősséggel.

26. A társaság adatvédelmi tisztviselője feladatköre keretében:
a) ellátja a társaság adatvédelmi tevékenységének irányítását, tájékoztat, szakmai tanácsot, iránymutatást ad;
b) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
c) felkérésre ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
d) kivizsgálja a hozzá érkezett bejelentéseket és adatvédelmi incidens észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót, indokolt esetben vizsgálat lefolytatását kezdeményezi a társaság vezetőjénél,

javaslatot tesz az incidens káros következményeinek elhárítására, a hasonló jövőbeni incidensek megelőzésére;

e) elkészíti az adatvédelem tárgyában kiadandó munkáltatói szabályzatok tervezetét, közreműködik az adatvédelmet érintő egyéb szabályzatok kidolgozásában. Segíti az ügyvezetőt az adatkezelésekre vonatkozó jogszabályok és szabályzatok érvényre juttatásában, ennek során figyelemmel kíséri az adatvédelemmel összefüggő jogszabályváltozásokat és jelzi a társaság vezetőjének a munkáltatói szabályzatok módosításának szükségességét;
f) közreműködik a társasággal jogviszonyban állók oktatásában és igény szerinti vizsgáztatásában;
g) egyedi ügyekben kidolgozott állásfoglalásával segíti az egységes gyakorlat kialakítását;
h) adatkezelési tevékenységét érintő ügyekben kialakítja a társaság álláspontját, kapcsolatot tart a NAIH-hal, közreműködik a NAIH vizsgálatainak lefolytatásában és az ezekkel összefüggő megkeresések megválaszolásában;
i) a kérelem tárgyában elkészíti az érintettnek a személyes adatai kezelésére vonatkozó kérelmére adandó válasziratokat;
j) gondoskodik a társaság honlapján megjelenített adatvédelmi nyilatkozat, irányelvek és adatkezelési tájékoztató naprakészen tartásáról;
k) peres ügyekben a társaság adatvédelemmel kapcsolatos álláspontját egyezteti a peres képviseletet ellátó személlyel. Az adatvédelemmel kapcsolatos perekben szakértőként vehet részt;
l) a társaság vezetője részére igény esetén éves összefoglalóban értékeli a társaság adatvédelmi tevékenységét;
m) adatvédelmi szempontból véleményezi a személyes adatokat tartalmazó informatikai nyilvántartásokra, szoftverekre vonatkozó fejlesztési javaslatokat;
n) feladat- és hatáskörében – a célhoz kötöttség elvére figyelemmel – jogosult a társaságnál folytatott adatkezelésekbe betekinteni, az adatkezelőtől felvilágosítást kérni;
o) ellenőrzi a GDPR-nak, valamint az egyéb uniós és tagállami adatvédelmi rendelkezéseknek, jelen belső szabályzatnak való megfelelést, képzést, auditokat;
p) közreműködik a betekintési és hozzáférési jogosultságok felügyeletében;
q) szakmai tanácsot ad a hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését.
r) ellenőrzi az adatfeldolgozók adatfeldolgozói szerződésben vállalt kötelezettségeinek betartását, amennyiben szerződésbe ütköző gyakorlatot tapasztal, ezt jelzi a társaság vezetőjének, javaslatot tesz a szerződéses kapcsolat megszüntetésére.

III. RÉSZ

A személyes adatok védelme a társaságnál

7. Az adatkezelés alapvető szabályai

27. A társaságnál kezelt adatállományt 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.

28. A társaság valamennyi adatkezelése vonatkozásában az adatállomány biztonsága érdekében köteles érvényre juttatni a Szabályzatban és más belső szabályozóiban és más dokumentumokban (folyamatokban, munkaszerződésekben, munkaköri leírásokban) és vezetői intézkedésekben meghatározott technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR és az Infotv., érvényre juttatásához szükségesek.

29. Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét, jogaik gyakorlásának lehetőségét.

30. Az adatállományhoz való hozzáférést a társaság, elektronikus úton (hálózati meghajtó, beléptető rendszer) jogosultsági szintek megadásával korlátozza.

31. A folyamatban levő munkavégzés, feldolgozás alatt levő iratokhoz csak az érintett ügyintézők férhetnek hozzá, a bér- és munkaügyi, illetve egyéb személyes adatokat tartalmazó iratokat biztonságosan elzárva – zárható irodákban és zárható szekrényekben – kell tartani.

32. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról. A társaság a tudomány és technológia állása és a megvalósítás költségei, az adatkezelés jellege hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett kockázat figyelembevételével köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi elvek, szabályok és az érintettek jogainak védelmére vonatkozó garanciák érvényre juttatásához szükségesek. Több lehetséges adatkezelési megoldás közül lehetőség szerint azt kell választani, amely az adatállomány magasabb szintű védelmét biztosítja.

33. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

8. Az adatvédelem alapvető szabályai

34. Az adatállomány kezelésének helyszínéül szolgáló épület megfelelő fizikai, és tűzvédelméről gondoskodni kell. Az adatállomány kezelése zárható helyiségébe csak az arra jogosultak léphetnek be.

35. Az informatikai rendszerek tűzfalas védelméről, vírusvédelméről, az adattárolókon lévő adatállomány biztonsági mentéséről, jelszavas védelméről, a mobil adathordozók titkosításáról, az informatikai rendszer naplózásáról a társaság gondoskodik.

36. Meghatározott adatkezelést nem végző dolgozó (pl. takarító, karbantartó) az adatállománnyal nem kerülhet kapcsolatba, ezért az ilyen tartalmú dokumentumokat

zárható szekrényben kell őrizni, a monitorok rálátásvédelméről, az informatikai eszköz őrizetlenül hagyása esetén a kijelző zárolásáról és jelszavas védelméről gondoskodni kell.

37. A társaság azon munkavállalói, akik az adatállomány meghatározott csoportját nem kezelik (pl. alkalmazotti adatok, alkalmazottak pénzügyi adatai, ügyféladatok), vagy meghatározott személyekre vonatkozó (pl. nem az adott ügyintéző ügyfele) személyes adatokat nem kezelik, azokhoz nem férhetnek hozzá.

38. A társaság elektronikus adatkezelésre, nyilvántartásra alkalmazott szoftvere lehetővé teszi a rendszer naplózhatóságát, hogy azonosítható legyen, mely felhasználó, mikor, mit rögzített, vagy törölt. A társaság, csak jogtiszta szoftvereket alkalmaz, beszerzi az alkalmazott szoftverekre vonatkozó hatásvizsgálati dokumentációt.

39. A társaság a hardverek esetén a garanciális időszakot követően új adathordozókat szerez be, és a garanciális időszakot meghaladott adathordozókat megsemmisíti, vagy biztonságosan törli.

40. A társaság gondoskodik mind az elektronikus, mind a papír alapú bejövő és kimenő kommunikáció ellenőrzéséről, vírusmentesítéséről. Adatállományt érintő adat elektronikusan kizárólag adathordozón, vagy titkosított csatornán, illetve jelszavas védelemmel továbbítható. A társaság adatkezeléssel kapcsolatos fontosabb folyamatait jelen szabályzat mellékletét képező **folyamatábrák** nevű mappa tartalmazza.

41. A jelszavak használata esetén ügyelni kell arra, hogy egymás jelszavát nem ismerhetik meg a felhasználók. A különböző informatikai rendszerekbe eltérő, megfelelően erős jelszót szükséges használni. A jelszavakat megfelelő jelszótároló programban indokolt tárolni. A jelszavakat negyedévente meg kell változtatni.

42. A szkennelésnél ügyelni kell arra, hogy minden felhasználó a saját mappájába tudja menteni az adatállományra vonatkozó dokumentumokat. Közösen használt nyomtató esetén biztosítani kell, hogy a nyomtatni kívánt dokumentum, a nyomtató személy jelenlétében jelenjen meg.

43. Az adatállományt megjelenítő képernyők, monitorok rálátásvédelméről a társaság vezetője gondoskodik. A felügyelet nélkül hagyott informatikai eszközök esetén 1 perc várakozás után automatikus képernyőzárolással szükséges ellátni.

44. Az informatikai rendszerekhez megfelelő azonosítás, hitelesítést követően lehet hozzáférni, a saját felhasználói adatok használatával.

45. Informatikai eszköz elvesztése esetén gondoskodni kell az alkalmazásokhoz való hozzáférések visszavonásáról, az adatok távoli törléséről.

46. Az informatikai rendszerek, alkalmazások sérülékenységi vizsgálatát bevezetését megelőzően el kell végezni.

47. A társaság felhőszolgáltatás igénybevétele esetén olyan szolgáltatót választ, amelynek tárhelye az Európai Unió valamely országában található.

48. A társaság eszközein a felhasználónevek, jelszavak megjegyzése nem állítható be. Jelszó papír alapon nem tárolható.

49. A társaság honlapjára közzétett fájloknál előzetesen a közzétevő személynek minden esetben ellenőrizni kell, hogy tartalmaz-e személyes, illetve egyéb védendő adatot. Amennyiben az anonimizálás nem lett elvégezve azt haladéktalanul jelzi a feladónak. A honlapon csak anonimizálást követően tehető közzé bármilyen dokumentum.

9. A társaság adatkezelési tájékoztatója

50. A Társaság általános adatkezelési tájékoztatóját az **adatkezelési tájékoztatók mappa** tartalmazza.

51. Amennyiben a társaság eseti adatkezelést végez (pl. rendezvény szervezése, álláshirdetés) úgy a vonatkozó tájékoztató kidolgozásáról és az érintettek részére elérhetővé tételéről megfelelően gondoskodik.

IV. RÉSZ
AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI

52. A Társaság valamennyi adatkezelése során biztosítja az érintett jogainak főszabály szerint díjmentes gyakorlását.

10. Az érintett hozzájárulása

53. Amennyiben a személyes adatok kezelése hozzájáruláson alapul, az érintett hozzájárulását úgy kell beszerezni, hogy a Társaság igazolni tudja, hogy a hozzájárulás előtt az érintettet a GDPR-ban előírt módon tájékoztatta az érintetett az adatkezelésről. A hozzájárulás önkéntességét biztosítani kell.

54. Hozzájárulásnak minősül az is, ha az érintett a társaság honlapjának megtekintése során bejelöl egy erre létrehozott négyzetet, amely az adott összefüggésben az érintett önkéntes, tájékoztatáson alapuló hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

55. A hozzájárulás az ugyanazon cél vagy célok érdekében történő összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra külön-külön meg kell adni.

56. Ha az érintett hozzájárulása más ügyekre is vonatkozik – így különösen értékesítési, szolgáltatási szerződés megkötése - a hozzájárulást ezektől a más ügyektől egyértelműen megkülönböztethető módon kell kifejezni, érthető és könnyen hozzáférhető formában,

világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó nyilatkozat bármely olyan része, amely a GDPR-ba ütközik, kötelező erővel nem bír.

57. A Társaság nem kötheti szerződés megkötését, teljesítését olyan személyes adatok szolgáltatása feltételéül, amelyek nem szükségesek a szerződés teljesítéséhez.

58. A hozzájárulás visszavonását azonos módon kell lehetővé tenni, mint annak megadását. A hírlevéről történő leiratkozás érdekében valamennyi hírlevél végén egy linkben biztosítani kell a hozzájárulás visszavonásának lehetőségét.

59. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a hozzájárulás visszavonását követően más jogalap szerint főszabály szerint nem kezelheti az adatokat.

60. A társaságnak bármikor igazolnia kell tudni azt, hogy az adatkezelési művelethez az érintett hozzájárult.

11. Szerződés, mint jogalap

61. A szerződés előkészítése során, a tervezet kidolgozásakor, véleményezésre megküldése során személyes adat feltüntetésére nem kerülhet sor.

62. A szerződésben csak a szerződés érvényességéhez és a teljesítéséhez szükséges személyes adatok kezelhetőek.

63. A szerződésekben külön adatvédelmi záradékot **(Adatfeldolgozói, közös adatkezelés szerződések)** szerint kell feltüntetni, amiben rögzíteni kell a papír alapú, illetve az elektronikus védelmi intézkedéseket a szerződésben szereplő személyes adatok védelme érdekében.

64. A szerződésben szereplő személyes adatok kezelésére a szerződés hatálya ideje alatt történhet. A szerződés teljesítését, megszűnését követően 5 évig az esetlegesen szerződésen alapuló követelések kölcsönös bizonyítása, érvényesítése érdekében is sor kerülhet. Amennyiben a szerződésben nyújtott jótállás a szerződés teljesítését követő 5 éven túli időre kiterjed, úgy a jótállási idő leteltét követő 5 évig jogszerűen kezelhetők a szerződésben szereplő személyes adatok.

65. A társaság a szerződést kötő partnerét tájékoztatja jelen szabályzatban meghatározott, szerződéskötéshez kapcsolódóan lényeges adatkezelési, adatvédelmi feltételekről.

12. Jogi kötelezettség teljesítése

66. A jogi kötelezettségen alapuló adatkezelés szabályaira – adatkezelés célja, kezelhető adatok köre, tárolás időtartama, címzettek – a vonatkozó jogszabály rendelkezései irányadók.

67. A jogi kötelezettség teljesítésén alapuló adatkezelés az érintett hozzájárulásától független. Az érintettel az adatkezelés megkezdése előtt ezesetben közölni kell, hogy az adatkezelés

kötelező, továbbá az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a rá vonatkozó jogi kötelezettség alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

13. Adatkezelő jogos érdeke

68. Az újságírási célú adatkezelés jogalapja főszabályként a jogos érdek.

69. A jogos érdek jogalapjának alkalmazása során az érintett személyes adatainak kezelése az érintett hozzájárulása nélkül történik, ezért garanciális jelentőségű, hogy az adatkezelő alaposan feltérképezze azt, hogy a tervezett adatkezelés az érintett információs önrendelkezés jogára milyen kihatással lesz, különösen online nyilvánosság esetén. Az érdekmérlegelést el kell végezni a tervezett adatkezelés megkezdése előtt és amennyiben érintetti joggyakorlás keretében az érintett tiltakozik az adatkezelés ellen, az adatkezelő kötelezettsége, hogy erre egy kifejezetten az érintettre szabott egyéni, megismételt érdekmérlegelés lefolytatásával reagáljon.

70. A sajtótermékek által személyes adatokat tartalmazó cikk publikálása során az érdekmérlegelésnek a konkrét közlés sajátosságait is figyelembe kell vennie, azokra külön reflektálnia kell. Az **érdekmérlegelési teszt mappában** található érdekmérlegelési teszt a sajtós adatkezelés sajátosságait figyelembe vevő teszt az egyes adatkezelések tekintetében mintaként, támpontként szolgál.

71. Az általános adatvédelmi rendelet 21. cikk (1) bekezdés szerint ugyanis az érintett a saját helyzetével kapcsolatos okból bármikor tiltakozhat személyes adatai kezelése ellen és ilyen esetben az adatkezelő köteles tulajdonképpen megismételni, de immár egyéniesített formában az érdekmérlegelési tesztet, mellyel igazolhatja, hogy az érintett jogaival, érdekeivel szemben az adatkezeléshez fűződő jogos érdekek elsőbbséget élveznek.

72. Személyes adat kezelhető abban az esetben is, amennyiben az adatkezelő, vagy egy harmadik fél jogos érdekében szükséges. A Társaság sajtó

73. Amennyiben a társaság jogos érdeke alapján kíván adatot kezelni, úgy előzetesen érdekmérlegelési tesztben szükséges felmérni az adatkezelés jogszerűségét, igazolva, hogy a társaság jogos érdeke megelőzi az érintettek személyes adatok védelméhez fűződő jogát.

74. A társaság képrögzítéssel járó kamerarendszert alkalmaz, amelynek részletes szabályairól külön szabályzat rendelkezik.

14. Személyes adatok gyűjtési céltól eltérő kezelése

75. Személyes adatok gyűjtési céljuktól eltérő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljával.

76. A közérdekű archiválási, tudományos, történelmi kutatási célból, vagy statisztikai célból történő további adatkezelés megengedett.

V. RÉSZ

MUNKAVISZONNYAL KAPCSOLATOS ADATKEZELÉSEK

15. Személyügyi nyilvántartás

77. A társaság megnevezés alatt jelen részben írtak esetén, a munkáltatót is érteni kell a munka törvénykönyvéről szóló 2012. évi I. törvény szerint (a továbbiakban: Mt.). A társaság az Mt-ben meghatározott adatkezelési alapelvek és szabályok figyelembevételével is kezeli az alkalmazottak adatait.

78. A társaság az alkalmazottak meghatározott személyes adatait, a munkavállalók adatkezelési tájékoztatójában meghatározott jogalap szerint és célból kezeli.

79. Az adatok pontosságának garantálása érdekében a munkavállaló a fenti adatokban bekövetkezett változást, 8 napon belül írásban köteles bejelenteni a társaság ügyvezetője részére.

80. A személyes adatok címzettjei, a munkáltató vezetője, munkáltatói jogkör gyakorlója, a társaság munkaügyi feladatokat ellátó munkavállalói és adatfeldolgozói. A társaság tulajdonosai részére csak a vezető állású munkavállalók személyes adatai továbbíthatók.

81. A munkavállaló köteles a munkája során tudomására jutott üzleti, szakmai titkot megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése a társaságra vagy más személyre hátrányos következménnyel járhat.

82. A betegségre, üzemi tanácsi, szakszervezeti tagságára vonatkozó adatokat a társaság csak az Mt-ben meghatározott jog, vagy kötelezettség teljesítése céljából kezelhet.

83. A személyes adatok tárolásának maximális időtartama: az öregségi nyugdíjkorhatárt követő 5 év lehet. A személyes adatokat irattárban, a jogosulatlan hozzáférés, megsemmisülés ellen védve kell tárolni.

84. A társaság a munkaszerződés megkötésével egyidejűleg a jelen szabályzat mellékletét képző" **Munkavállalók**" elnevezésű mappában található, adatkezelési tájékoztató megismertetésével tájékoztatja a munkavállalót személyes adatainak kezeléséről és a személyhez fűződő jogokról.

85. A foglalkoztatásra irányuló jogviszonnyal kapcsolatos személyi irat, dokumentum kizárólag személyesen, vagy meghatalmazott útján vehető át, illetve tértivevényes ajánlott küldeményként az érintett lakcímére postázandó.

86. A társaság foglalkoztatottjai kötelesek a feladatkörükben tudomásukra jutott személyes adatokat, üzleti, szakmai titkokat, szellemi termékeket, ügyintézéshez kapcsolódó más érzékeny információkat megőrizni. Az adatkezelő ennek érdekében a munkavállalókkal a munkaszerződés kiegészítése nevű dokumentumot íratja alá.

87. A társaság nem jogosult az alkalmazotti okmányainak másolására, amennyiben erre jogszabály nem hatalmazza fel.

88. A személyi anyagba csak az arra jogosultak tekinthetnek be, a betekintés tényét, idejét és a betekintő nevét a személyi anyagban **betekintő lapon** dokumentálni kell, amely a **Betekintési napló** mappában található.

16. Alkalmassági vizsgálatokra vonatkozó adatkezelés

89. A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

90. A pszichológiai vagy személyiségjegyeket kutató tesztlapokat, az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében kitöltethető a munkavállalók nagyobb csoportjával, de csak akkor, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.

91. A munkavállalót előzetesen tájékoztatni kell, hogy az adott munkakör betöltésére csak megfelelő készség, képesség esetén van lehetőség.

92. A vizsgálat előtt részletesen tájékoztatni kell a munkavállalókat arról is, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel, gyakorisággal történik, ki végezheti, eredménye milyen hatással lesz jogaikra, a személyes beavatkozás lehetősége fennáll-e, automatikus döntéshozatalra, profilalkotásra sor kerül-e. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabályi rendelkezésről is. E Tájékoztatáshoz kapcsolódó adatkezelési tájékoztató mintáját jelen szabályzat a **Munkavállalók"** elnevezésű mappában, Tájékoztató alkalmassági vizsgálatról nevű dokumentum tartalmazza.

93. A munkaalkalmasság, felkészültség mérésére irányuló tesztlapokat a tájékoztatást követően a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal. A tesztlapok kitöltése nem irányulhat a munkavállalók zaklatására, jogaik csorbítására.

94. A munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor tölthető ki a munkavállalók nagyobb csoportjával pszichológiai, vagy személyiségjegyek

kutatására alkalmas tesztlap, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.

95. A kezelhető személyes adatok köre a munkaköri alkalmasság ténye, és az ehhez szükséges feltételek megállapítása. Az adatkezelés jogalapja: a munkáltató jogos érdeke. A személyes adatok kezelésének célja munkaviszony létesítése, fenntartása, munkakör betöltése.

96. A vizsgálati eredményt az érintett munkavállalók, illetve a vizsgálatot végző, titoktartási kötelezettség alá eső szakember ismerheti meg. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját a munkáltató nem ismerheti meg.

97. A személyes adatok a jogviszony megszűnését követő 5 évig kezelhetőek. A teszteket, és a munkavállalókra vonatkozó értékeléseket a személyi anyagtól elkülönítve kell, elzártan tárolni.

98. Az elektronikus levelezőrendszer, az informatikai eszközök, a munkahelyi internethasználat és a céges mobiltelefon használatának ellenőrzésével kapcsolatos szabályok az informatikai biztonsági szabályzatban kerülnek rögzítésre.

VI. RÉSZ

ADATVÉDELMI INCIDENSEK KEZELÉSE

17. Az adatvédelmi incidens fogalma

99. Az adatvédelmi incidens fogalmát a GDPR 4. cikk 12. pontja tartalmazza. Adatvédelmi incidens lehet például: a pendrive, laptop vagy mobil telefon elvesztése, személyes adatok elvesztése, nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása (tévesen küldött email), ügyfél- és vevő- partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése, személyes adatot kezelő informatikai rendszer elérhetetlenné válása, személyes adat nyilvánosságra hozatala.

18. Adatvédelmi incidensek kezelés, orvoslása

100. Az adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása, ellenőrzése a társaság vezetőjének feladata.

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

102. Amennyiben a társaság ellenőrzésre jogosult munkavállalói adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell a társaság vezetőjét.

103. Az adatvédelmi incidens bejelenthető a társaság központi e-mail címén, telefonszámán.

104. Adatvédelmi incidens kezelésére, orvoslására külön szabályzat vonatkozik.

19. Nem belső adatvédelmi incidens

105. Amennyiben a Társaság elérhetőségeinek bármelyikén olyan információkhoz jut, megkeresések érkeznek hozzá, amely során egyértelmű, hogy a személyes adatokkal kapcsolatban nem merül fel adatkezelési tevékenysége (pl. rossz címre küldött csomag, boríték, elektronikus levél, stb.), úgy ezen incidenseket során az alábbiak szerint jár el:

a) az adatvédelmi incidensről nyilvántartást vezet, ezt a szabályzat 5. számú melléklete képezi
b) haladéktalanul megteszi a szükséges lépéseket az incidens elhárítására (pl. csomag visszaküldése, feladónak visszajelzés jelzés),
c) az érintettet erről tájékoztatja;
d) a birtokába jutott személyes adatokat semmilyen célból nem kezeli.

VII. RÉSZ

ADATVÉDELMI HATÁSVIZSGÁLAT

20. Adatvédelmi hatásvizsgálat és előzetes konzultáció

106. Ha az adatkezelés figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, különösen, ha a NAIH által nyilvánosságra hozott hatásvizsgálati listában szereplő következő adatkezelésre vonatkozik (https://www.naih.hu/hatasvizsgalati-lista):

1. Ha egy természetes személy **biometrikus adatainak** kezelése módszeres megfigyelésre irányul.
2. Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos **biometrikus adat** kezelése történik.
3. Ha az adatkezelés egy természetes személy **genetikai adatainak** egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.
4. Ha egy természetes személy **genetikai adatai** kezelésének célja a természetes személy értékelése vagy pontozása1[1].
5. **Pontozás.** Az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.

6. **Hitelképesség értékelése.** Az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
7. **Fizetőképesség értékelése.** Az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagy számú, illetve módszeres értékelése útján.
8. **Harmadik személytől gyűjtött adatok további felhasználása.** Az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
9. **Diákok, hallgatók személyes adatainak értékelésre való felhasználása.** Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.
10. **Profilozás.** Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.
11. **Csalás elleni fellépés.** Az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
12. **Okosmérők.** Az adatkezelés célja közműszolgáltatók által telepített „okosmérők" alkalmazása (fogyasztási szokások nyomon követése).
13. **Joghatással** vagy **hasonló jelentős hatással** járó **automatizált döntéshozatal.** Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
14. **Módszeres megfigyelés.** Érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).
15. **Helymeghatározási adatok** kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
16. **Munkavállaló munkájának megfigyelése.** Munkavállalók munkájának megfigyelése. Az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése.2[2] Például GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából.
17. **Különleges adatok nagy számban való kezelése.** A GDPR (91) preambulumbekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.
18. **Nagyszámú személyes adatok kezelése bűnüldözési célból**
19. **Kiszolgáltatott helyzetben** lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: pl. gyermekek, idősek, mentális betegségben szenvedők esetében.

20. **Gyermekek** személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy **marketing céljából**, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.
21. **Új technológiai** megoldások használata az adatkezelés során. Ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelése (pl.: okos televízió, okos háztartási eszközök, okos játékok stb.), és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.
22. **Egészségügyi adatokra vonatkozó adatkezelések.** Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelése.
23. Amikor több adatkezelő **egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot** tervez létrehozni, amelyben különleges adatokat is kezelnek.
24. Az adatkezelés célja a különböző forrásokból származó adatok **összevonása,** egymással való **megfeleltetése** vagy **összehasonlítása.**

akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

107. Nem kell adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges vagy közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az adatkezelést jogszabály írja elő, amennyiben a jogalkotó a jogszabály-előkészítés során adatvédelmi hatásvizsgálatot végzett.

108. Az adatvédelmi hatásvizsgálat szükségességének megállapításához az 1. függelékben foglalt kérdéseket szükséges megválaszolni.

109. Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az ügyvezető, vagy általa megbízott személy rögzíti.

110. Amennyiben az ügyvezető által megbízott személy az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, adatvédelmi hatásvizsgálat lefolytatását kezdeményezi az ügyvezetőnél.

111. Az ügyvezető az érintett szakterület javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását, vagy írásban rögzíti mellőzésének okait. Az adatvédelmi

hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

112. Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelés által érintett szakterület vesz részt. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő és az elektronikus információs rendszer biztonságáért felelős személy segíti. Az adatvédelmi hatásvizsgálat iratai nem nyilvánosak.

113. Az adatkezelési hatásvizsgálatot végző az adatvédelmi hatásvizsgálatról összefoglaló értékelést készít a 2. függelékben foglaltak figyelembevételével. Az összefoglaló értékelést az adatkezelő szerv vezetője hagyja jóvá, melyet követően az adatkezelést el lehet kezdeni.

114. A hatásvizsgáltot a NAIH honlapján elérhető hatásvizsgálati szoftver (PIA szoftver) alkalmazásával kell teljesíteni.

115. Az adatvédelmi hatásvizsgálat megrendeléséért a társaság vezetője a felelős. A hatásvizsgálatba, ha van kijelölt adatvédelmi tisztviselő, tanácsát ki kell kérni.

116. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal.

117. Az adatvédelmi hatásvizsgálat és előzetes konzultáció részletes szabályaira a rendelet 35-36. cikkei és az Infotv. rendelkezései irányadók.

XIV. RÉSZ

AZ ADATTOVÁBBÍTÁS SZABÁLYAI

21. Adatkezeléssel, adattovábbítással megbízott dolgozók

118. Az adatok kezelésére vonatkozó megbízás nem foglalja magában az adattörlés, adatmódosítás, adattovábbítás, közzététel jogának egyedüli gyakorlását. Az adattörlés, adatmódosítás, adattovábbítás, közzététel teljesítéséhez minden esetben vezetői – ügyvezető, vagy helyettese – jóváhagyás szükséges.

119. Az adatok felvételével, nyilvántartásával megbízott dolgozók a munkaköri leírásukban szereplő feladatokkal kapcsolatosan az alkalmazottak adatait felvehetik, nyilvántarthatják:
- ügyvezető
- megbízott munkatárs

120. A ügyfelek adatait felvehetik, nyilvántarthatják, továbbíthatják:
- ügyvezető
- megbízott munkatárs

121. A társaság által kezelt adatok szabályszerű megkeresés esetén továbbíthatók az adatok kezelésére jogosult hatóságok, bíróságok részére az ügyvezető jóváhagyását követően.

22. Hatósági megkeresések

122. Személyes adatot érintő adatszolgáltatást kizárólag az ügyvezető beleegyezésével lehet teljesíteni. Személyes adatot hatósági, bírósági **megkeresés alapján** az ügyvezető, míg a NAIH megkeresése alapján az adatvédelmi tisztviselő jogosult kizárólag írásban és csak akkor **kiadni**, ha

a) a megkeresés papír alapon kiadmányozott, hivatalos postai küldeményként feladott, vagy elektronikusan kiadmányozott cég kapura érkezett, és

b) a megkereső szerv a megkeresésben megjelölte azt a személyt, akiről a fentiekben meghatározott szerv, vagy hatóság a személyes adat kiadását kéri, valamint a kért adatok fajtáját, az adatkérés célját és a teljesítés határidejét.

123. Amennyiben a megkeresés az előző pontban írtaknak nem felel meg (pl. telefonon, e-mailben érkezik) fel kell hívni a megkeresés szabályszerű előterjesztésére. Amennyiben a megkereső kiléte kétséges, a megkeresés jogszerűségéről szükséges meggyőződni (pl. a megkereső szerv ügyintézőjének telefonos megkeresése útján).

124. Az adatot ki kell adni, amennyiben a feladatkörében eljáró hatóság szabályszerű helyszíni ellenőrzést folytat és a dokumentum az ellenőrzés lefolytatásához szükséges. Szabályszerű a **helyszíni ellenőrzés**, ha

a) az ellenőrök az ellenőrzést megelőzően átadják megbízólevelüket, amely tartalmazza a megbízó nevét, az ellenőrzés tárgyát, időszakát, és a megbízott ellenőr azonosító adatait, és

b) az ellenőrök igazolják a megbízó levél alapján személyazonosságukat.

125. Kivételesen (különösen indokolt esetben) akkor is teljesíthető a hatósági, bírósági megkeresés, ha papír alapon nem áll rendelkezésre a megkeresés eredeti példánya (például mert a megkeresés a nyomozati cselekmények sürgőssége miatt telefaxon érkezett). Ez esetben is feltétele a megkeresés teljesíthetőségének az egyéb feltételek megléte.

126. A megkeresés akkor teljesíthető, ha

a) a kért adatokat a társaság jogszerűen kezeli,

b) a kért adatok kezelésére a megkereső fél is jogosult

c) az adatok rendelkezésre állnak (amennyiben nem közhiteles nyilvántartásból történik az adatszolgáltatás, ennek tényére a válaszban szükséges utalni)

d) a megkeresés biztonságosan teljesíthető (pl. titkosított e-mail keresztül)

23. Külföldi adattovábbítás

127. A társaság bizonyos adatkezelések (pl. felhőtárhely szolgáltatás igénybe vétele) esetében személyes adatokat továbbíthat az Európai Gazdasági Térségen kívüli harmadik országba, vagy nemzetközi szervezet részére (továbbiakban: külföldi adattovábbítás), ezek

felmerülése esetén előzetesen pontosan tisztázni kell, hogy adattovábbítás történik-e harmadik országba, vagy nemzetközi szervezet részére.

128. A külföldi adattovábbításra akkor kerülhet sor, ha az Európai Unió Bizottsága (továbbiakban: Bizottság) megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít a személyes adatok számára (továbbiakban: megfelelőségi határozat).[3]

129. Megfelelőségi határozat hiányában a társaság csak abban az esetben továbbíthat személyes adatokat, ha a címzett adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújt az adatok kezelésével kapcsolatban. Ilyen megfelelő garanciák lehetnek - az illetékes felügyeleti hatóság külön engedélye nélkül - például:

a) a Bizottság által elfogadott általános adatvédelmi kikötések, illetve a felügyeleti hatóság által elfogadott és a Bizottság által jóváhagyott általános adatvédelmi kikötések;
b) jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat;
c) jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

130. Megfelelő garanciák hiányában az alábbi feltételek valamelyikének teljesülése esetén történhet adattovábbítás:

a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról;
b) az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
c) az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
d) az adattovábbítás fontos közérdekből szükséges;
e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
g) a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

---

[3] Andorra, Argentína, Feröer Szigetek, Guernsey, Izrael, Jersey, Kanada, Man-sziget, Svájc, Uruguay, USA, Új-Zéland

131. Ha az adattovábbítás nem alapulhat megfelelőségen, nem állnak rendelkezésre megfelelő garanciák és a különleges helyzetekre vonatkozó eltérések egyike sem alkalmazandó, akkor a harmadik országba történő adattovábbítás csak akkor történhet, ha:

a) az adattovábbítás nem ismétlődő,
b) csak korlátozott számú érintettre vonatkozik,
c) az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és
d) az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében.

132. Ilyen esetekben a társaságnak tájékoztatnia kell a NAIH-ot az adattovábbításról. Az adatkezelő az általános tájékoztatási kötelezettségén túlmenően, az érintettet tájékoztatja az adattovábbításról, valamint az adatkezelő kényszerítő erejű jogos érdekéről.

XII. RÉSZ

AZ ÉRINTETT JOGAI

24. Tájékoztatás az érintett jogairól

133. Az általános adatvédelmi rendelet 21. cikk (4) bekezdése alapján az (1) és (2) bekezdésben említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

134. A társaság honlapján az érintettek jogairól tájékoztatót kell elhelyezni és azt folyamatosan karbantartani, amely az Ügyfelek mappában található.

135. Az adatkezeléshez kapcsolódó igényeket a társaság vezetője részére be kell mutatni, aki gondoskodik azok határidőn belüli megválaszolásáról.

136. Minden esetben meg kell győződni arról, hogy a jogokat gyakorolni kívánó személy jogosult-e a jogok gyakorlására. Ebből a célból az érintettnek a jog gyakorlásához kapcsolódó személyes adatait előzetesen ellenőrizni kell. Az azonosítás során csak az azonosítás teljesítéséhez szükséges adat kezelhető.

137. A jogok gyakorlása során mások jogai, szabadságai nem sérülhetnek, ezért a társaság a meg nem ismerhető adatok anonimizálásáról gondoskodik.

138. A társaság annak érdekében, hogy az érintett a jogait megfelelő módon és terjedelemben gyakorolhassa, az adatvédelmi tisztviselőt bevonja az érintettnek adandó választervezet előkészítésébe.

139. Az érintett jogait díjmentesen gyakorolhatja. A visszaélésszerű joggyakorlás esetén – így különösen ugyanarra az adatra vonatkozó ismételt kérelem esetén – önköltségi díj számítható fel.

140. Az érintetti joggyakorlás elősegítésére a társaság külön szabályzatot alkalmaz.

141. Az érintett jogai:
a) átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának elősegítése;
b) előzetes tájékozódás – ha a személyes adatokat az érintettől gyűjtik;
c) az érintett tájékoztatása, ha a személyes adatait nem tőle szerezték meg;
d) hozzáférési jog;
e) helyesbítéshez való jog;
f) törléshez való jog (elfeledtetéshez való jog);
g) adatkezelés korlátozásához való jog;
h) a helyesbítéséhez, törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítés joga;
i) adathordozhatósághoz való jog;
j) tiltakozáshoz való jog;
k) automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást;
l) korlátozások;
m) tájékoztatás az adatvédelmi incidensről;
n) a felügyeleti hatóságnál panaszhoz való jog (hatósági jogorvoslathoz való jog);
o) a felügyeleti hatósággal szembeni bírósági jogorvoslat joga;
p) az adatkezelővel vagy az adatfeldolgozóval szembeni bírósági jogorvoslat joga;

25. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának támogatása

142. Az adatkezelő az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és tájékoztatást díjmentesen, tömör, átlátható, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel megfogalmazva kell nyújtania, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – dokumentáltan kell megadni, az adatfelvételt megelőzően. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

143. Az adatkezelőnek elősegíti az érintett jogainak a gyakorlását, ennek biztosítása érdekében konzultál az adatvédelmi tisztviselővel.

144. Az adatkezelő indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről. E határidő a GDPR-ban írt feltételekkel további két hónappal meghosszabbítható. A határidő meghosszabbításáról és annak okairól az érintettet egy hónapon belül tájékoztatni kell.

145. Ha az adatkezelő nem intézkedik az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

146. Az adatkezelő az információkat és az érintett jogairól szóló tájékoztatást és intézkedést díjmentesen biztosítja, azonban ha kérelme egyértelműen megalapozatlan, vagy túlzó, az adminisztratív költségekkel egyező összegű díjat számíthat fel.

147. Az érintetti jogok az érintett megfelelő azonosítását lehetővé tevő akár személyesen, akár elektronikusan, akár postai úton előterjesztett kérelemnek az Adatkezelőhöz történő eljuttatásával gyakorolhatók. Az érintett személyesen, hétfő 7:30 – 17:00 kedd szerda csütörtök 7:30 – 15:30 péntek, 7:30 – 11:30 óra között hangrögzítés nélkül gyakorolhatja jogait. Az adatkezelő az igénybejelentéstől számított legrövidebb időn, de legfeljebb 1 hónapon belül a kérést kivizsgálja, és írásos tájékoztatót nyújt.

148. Az érintett jogainak megsértése, ill. észrevétel esetén az alábbi elérhetőségeken tehet nyilatkozatot, ill. az alábbi hatóságokhoz fordulhat:

149. Az érintett jogainak megsértése, ill. észrevétel esetén Az Adatkezelő felé valamint az alábbi hatóságokhoz fordulhat a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat.

XIII. RÉSZ

ZÁRÓ RENDELKEZÉSEK

26. A Szabályzat megállapítása, módosítása és beépítése

150. A Szabályzat megállapítására és módosítására a társaság vezetője jogosult.

151. Jelen szabályzatot a társaságnál helyben szokásos helyen és módon ismertetni kell a munkavállalókkal, a szerződéses partnerek részére igény esetén meg kell küldeni, át kell adni.

152. Jelen szabályzat a társaságnál helyben szokásos helyen és módon történt kihirdetést követő napon hatályba lép.

153. A szabályzatot a jogszabályi környezet, a NAIH joggyakorlatának jelentős változása, a társaság tevékenységében, adatkezeléseiben bekövetkező jelentős változás esetén soron kívül, egyéb esetben 3 évente felül kell vizsgálni.

154. A társaság vezetője gondoskodik arról, hogy az adatvédelmi szabályzatban meghatározott előírások a társaság folyamataiban és mindennapjaiban érvényre jussanak.

155. Jelen szabályzatban foglaltak betartása és érvényesítése a társaság valamennyi munkavállalójának kötelessége.

156. Jelen szabályzatot valamennyi munkavállaló számára elérhetővé kell tenni, mind elektronikusan, mind papír alapon.

157. A Szabályzat rendelkezéseit meg kell ismertetni a társaság valamennyi munkavállalójával (foglalkoztatottjával), és a munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden munkavállaló (foglalkoztatott) lényeges

munkaköri kötelezettsége. A munkaszerződés kiegészítés mintáját a Munkavállalók nevű mappa tartalmazza.

158. A társaság jelen szabályzat alapján a munkavállalók munkaszerződéseit kiegészíti, a munkavégzéssel együtt nem járó személyes adatok átadása esetére titoktartási kötelezettséget ír elő.

159. A társaság az adatvédelmi szabályok megszegése esetén az érintettel szemben fegyelmi eljárást kezdeményez, indokolt esetben büntető feljelentést tesz.

160. A társaság állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, az adatvédelmi tisztviselő, vagy más erre megbízott személy köteles az állományba vételt követő 1 héten belül adatvédelmi oktatásban részesíti, egyidejűleg a vezetője a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátja.

161. A társaság személyes adatok kezelő állománya évente adatvédelmi oktatáson vesz részt, amelyet adatvédelmi tisztviselő tart.

162. Az érintett vezető, a rá vonatkozó adatvédelmi szabályok betartásáról és a hozzá tartozó állomány kapcsán a szabályok érvényesüléséről gondoskodik. Az érintett vezető a 1. sz. melléklet szakterületét érintő részét figyelemmel kíséri, a változást jelzi a nyilvántartásért felelős személy részére.

163. Az adatkezelő szerv adatvédelmi tevékenységének célellenőrzését az adatkezelő szerv vezetője rendelheti el. Az informatikai biztonsági feltételek teljesülését rendszeresen ellenőrizni kell, eredményéről tájékoztatni kell a vezetőt.

164. Jelen szabályzat és annak mellékletei dr. Kozma- Egeresi Gabriella e.v. szellemi terméke, aki fenntart minden jogot ideértve a fordítást, többszörözést, értékesítést is.

1. függelék kérdőív az előzetes kockázatelemzéshez

Első rész: Szükséges-e a hatásvizsgálat lefolytatása? Előzetes adatvédelmi kockázatelemzés

1. Használ vagy fejleszt-e olyan informatikai rendszert, amely személyes adatokat kezel?

Igen □ Nem □

2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?

Igen □ Nem □

3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévőszemélyes adatokkal kapcsolatban?

Igen □ Nem □

a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentő mértékben megváltoztatja az adatkezelést?

Igen □ Nem □

b) Ha releváns szervezeti változás következik be:

– az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?

Igen □ Nem □

– ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?

Igen □ Nem □

c) Ha ez az információ már korábban be lett gyűjtve:

– érint-e új vagy nagy létszámú érintett csoportot?

Igen □ Nem □

– rögzít-e ezen felül további személyes adatot?

Igen □ Nem □

4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?

Igen □ Nem □

5. Tervezi-e egymást követő 12 hónapból álló időszak során nagyszámú érintettekre vonatkozó személyes adatainak kezelését?

Igen □ Nem □

6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy munkavállalókra vonatkozó, széles körűnyilvántartási rendszerekben tárolt adatok kezelése?

Igen □ Nem □

7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentő mértékben érintőintézkedések épülnek?

Igen □ Nem □

8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?

Igen □ Nem □

9. Megvalósul-e nyilvánosság számára hozzáférhetőterületek (közterületek) nagyarányú, automatizált nyomon követése?

Igen □ Nem □

10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?

Igen □ Nem □

11. Az adatkezelő vagy adatfeldolgozó főtevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerűmegfigyelését igénylik?

Igen □ Nem □

12. A személyes adatokat olyan jelentő számú személy számára teszi-e hozzáférhetőé, amely észszerűn elvárható módon nem korlátozható?

Igen □ Nem □

13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőzőrendszer, például biometrikus azonosítás?

Igen □ Nem □

14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?

Igen □ Nem □

15. Megvalósul-e automatizált adatfeldolgozás?

Igen □ Nem □

16. Személyes adatok védelmének növelése érdekében elő́r-e (ha volt ilyen) a korábbinál magasabb szintűadatbiztonsági követelményeket?

Igen □ Nem □

17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?

Igen □ Nem □

18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?

Igen □ Nem □

19. Megvalósul-e tudományos kutatási vagy statisztikai célból történőadatkezelés?

Igen □ Nem □

20. Az adatkezelés kiterjed-e különleges adatokra?

Igen □ Nem □

21. Megvalósul-e bármilyen más, magánszférát érintőmagatartás?

Igen □ Nem □

22. Végeztek-e már korábban hatásvizsgálatot? Ha a válasz igen, csatolja a dokumentumot!

Igen □ Nem □

Második rész: Előzetes hatásvizsgálat

1. Ki a tájékoztatásra kötelezett személy (név, telefonszám, e-mail-cím)? (Ha van adatvédelmi tisztviselő, akkor az ő adatai.)

2. Mutassa be a szolgáltatás működését, felépítését!

3. Ki az adatkezelő (név, telefonszám, e-mail-cím, postai cím)?

4. Mi az adatkezelés pontos címe/helye/webhelye? (Csak akkor töltse ki, ha az eltér az adatkezelő címétől!)

5. Mi az adatkezelés célja, módja és jogalapja?

6. Mi az adatkezelés időtartama?

7. Kíván-e adatfeldolgozót igénybe venni? Ha igen, mutassa be részletesen az adatfeldolgozó személyét (kapcsolattartó, adatkezeléssel összefüggő tevékenység, adatfeldolgozó címe, adatfeldolgozás helye, technológiája stb.)!

8. Melyek a kezelni kívánt adatkörök?

9. Határozza meg a gyűjteni kívánt adatok mennyiségét, illetve az érintett személyek számát (hozzávetőlegesen)!

10. Melyek az adatfelvétel formái? Megvalósulhat az adatgyűjtés személy azonosítására alkalmas igazolvány segítségével is? Ha igen, fejtse ki!

11. Az adatszolgáltatás önkéntes? Ha igen, az érintettek megfelelő mértékben tájékoztatva vannak-e a kezelt adatok köréről, illetve jogaikról?

12. Az érintetteknek van-e lehetőségük arra, hogy adataik kizárólag meghatározott célokra történő felhasználásához nyújtsanak hozzájárulást? Ha igen, hogyan?

13. Megvalósul-e harmadik országba irányuló adattovábbítás? Ha igen, írja le a továbbítandó adatok fajtáit, a továbbítás címzettjének adatait, valamint az adattovábbítás jogalapját!

14. Fejtse ki, milyen lépéseket tesz az adatok biztonságának megőrzése érdekében!

15. Ha megfelelő szintűnek vélt az adatok biztonsága, milyen eszközök óvják az azonosítatlan hozzáféréstől?

16. A megfelelő védelmi eszközöket használja azonosítatlan hozzáférés megakadályozása érdekében? Fejtse ki álláspontját!

17. Van egyéb közlendő információja?

Harmadik rész: További analízis

1. Hogyan biztosítja az érintettek jogainak érvényesítését?

2. Fejtse ki azokat az Ön által is ismert, alternatív megoldásokat, amelyek az eredeti eljáráshoz képest a cél elérése mellett kisebb mértékben érintenék a magánszférát!

3. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?

4. Hogyan ellenőrzi az adatok teljességét?

5. Megfelelően naprakészek-e a gyűjtött adatok? Ha igen, támassza alá válaszát!

6. Kifejtett és részletezett az adatok természete?

7. Kinek van hozzáférési joga (lehetősége) a személyes adatokhoz?

8. Mi alapján kerülnek kiválasztásra azok a személyek, akik rendelkeznek ezzel a joggal?

9. A személyes adatokhoz való hozzáférés feltételei, módja, korlátai rögzítve vannak?

10. Milyen eszközök biztosítják az adatkezelés céljától eltérő felhasználás megakadályozását?

11. Hozzáférhet-e más rendszer a saját rendszerben kezelt adatokhoz? Ha igen, fejtse ki!

12. Az adatkezelés idejének lejárta után milyen módon kerülnek törlésre az adatok? Hogyan lesz dokumentálva az adattörlés

2. függelék az adatvédelmi hatásvizsgálatról szóló összefoglaló értékelés tartalmi elemei

1. A tervezett vagy megváltozott adatkezelés leírása:

A tervezett/megváltozott adatkezelés folyamatának leírása, melyben bemutatásra kerülnek az alábbiak:

a) adatkezelés jellege, hatóköre, körülményei;

b) a személyes adatok, a címzettek, valamint a személyes adatok tárolási időtartamának meghatározása;

c) funkcionális leírás az adatkezelési műveletről;

d) módszeres leírás az adatfeldolgozásról, az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

e) jogalap meghatározása;

f) a személyes adatokhoz használt eszközök (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) megnevezése;

g) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat;

h) az adatkezelésre vonatkozó, rendelkezésre álló igazgatási rendszerterv vagy folyamatleírás bemutatása;

i) hatásvizsgálatra vonatkozó szerep- és felelősségi körök meghatározása.

2. Az adatkezelési műveletek szükségességi és arányossági vizsgálata:

a) meghatározottak, kifejezettek és jogosak-e a cél(ok) [célhoz kötöttség elve – GDPR rendelet 5. cikk (1) bekezdés b) pontja];

b) az adatkezelés jogszerűsége (GDPR rendelet 6. cikk);

c) a kezelni kívánt adatok megfelelőek, relevánsak, és csak a szükséges adatokra korlátozódnak [adattakarékosság elve – GDPR rendelet 5. cikk (1) bekezdés c) pontja];

d) korlátozott tárolási időtartam [korlátozott tárolhatóság elve – GDPR rendelet 5. cikk (1) bekezdés e) pontja].

3. Meglévő vagy tervezett intézkedések: az adatkezeléssel összefüggő, a hatásvizsgálat elvégzésekor meglévő intézkedések felsorolása pl. jogosultságkezelés.

4. A jogokat és szabadságokat érintő kockázatok vizsgálata:

A kérdőívek kitöltése, valamint az érintettekkel történő esetleges konzultáció után a hatásvizsgálatot lefolytató szerv az adatkezelés minden releváns részelemének ismeretében elvégzi a kockázatkezelést, amelynek elemei az alábbiak:

a) a lehetséges kockázati tényezők azonosítása,

b) a kockázati tényezők értékelése,

c) a kockázati tényezők csökkentésére, megszüntetésére irányuló javaslatok megfogalmazása.

A kockázati tényezők azonosításában nagy szerepe van továbbá az érintettekkel való konzultációnak. A GDPR rendelet az érintettekkel való konzultációt nem szükségszerűen írja elő. Az adatkezelő „adott esetben" kéri ki az érintettek, illetve képviselőik véleményét. Ha az adatkezelő végleges döntése eltér az érintettek véleményétől, akkor dokumentumokkal alá kell támasztania annak végrehajtásának vagy elvetésének okait. Az adatkezelőnek dokumentumokkal kell indokolnia azt is, hogy miért nem kéri ki az érintettek véleményét, amennyiben úgy dönt, hogy erre nincs szükség.

4.1. Konzultáció az érintett szereplőkkel

Azonosítani kell az érintett szereplők lehetséges körét, majd megfelelő mértékben tájékoztatni kell őket az eljárásról. A tájékoztatás célja – a visszajelzések útján – a negatív hatások csökkentése, illetve a figyelem felhívása a jogorvoslati lehetőségre. A tájékoztatás során ki kell térni az eljárás menetére, idejére, várt eredményére. Az esetleges konzultációt már a tervezési/fejlesztési szakaszban célszerű elvégezni, hogy az érintettek észrevételeit, ajánlásait esetlegesen implementálni lehessen, jelentős többletköltség nélkül. Az érintetti kör nincs korlátozva, a projekt tárgyát tekintve érintett lehet állami és civil szervezet, támogató, szolgáltató, fejlesztő és az adatkezelés adatalanyai egyaránt.

Az érintettek hatásvizsgálatba való bevonásának lehetőségei:

– az egyes érintett kategóriák meghatározása és párbeszéd folytatása az egyes kategóriák képviselőivel;

– konzultációs eljárások biztosítása, hogy az érintetteknek lehetőségük legyen álláspontjaik kifejtésére;

– a tervezet érintettek számára történő hozzáférhetővé tétele.

A konzultáció formája többféle lehet: interjú, közvélemény-kutatás, meghallgatás, workshop, online konzultáció.

A tervezett adatkezelés negatív hatásainak csökkentése vagy kiküszöbölése érdekében célszerű a visszajelzéseket dokumentálni, és az adatkezelés megvalósítása során figyelembe venni.

4.2. A lehetséges kockázatok csoportjai

Személyeket érintő kockázatok:

– az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne;

– az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül;

– adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki;

– azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.

Szervezeteket érintő kockázatok:

– adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, amelynek következményeként bírság vagy más szankciók is kiszabhatók;

– olyan problémák felmerülése, amelyekre csupán a projekt elindítását követően derül fény, és a kijavításuk rendkívül költségigényes;

– az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti a projekt hatékonyságát;

– a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg;

– adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.

Jogi szabályozásnak való megfelelés vizsgálata:

– az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak, az ágazatspecifikus előírásoknak vagy az alkotmányjogi előírásoknak.

4.3. Az adatvédelmi kockázatok rangsorolása

Az elemzés az 1. függelékben szereplő kérdéssor alapján azonosított kockázatok és az érintett konzultáció értékelésével folytatódik. A magánszférára gyakorolt hatásuk mértéke alapján megkülönböztethető:

– alacsony (esély van a kockázat megjelenésére, de vannak enyhítő körülmények);

– közepes (valószínű, hogy megjelenik a kockázat, ha nem történik korrekció);

– magas (megjelenik a kockázat, ha nem történik korrekció) szintű kockázat.

Egy kockázat mértékét négy tényező befolyásolja:

A személyes adatkezelés alapját képező elektronikus információs rendszer kritikussága: nem kritikus = 1 kritikus = 2.

Az adatkezelés hatásköréhez tartozó adatokhoz képest (pl. az adott népesség aránya) az adatkezelés

1. kis számú = 1,

2. közepes = 2,

3. nagy számú = 3

érintett adatkezelését valósítja meg.

A kockázat elhárításának ügyviteli sürgőssége: a bejelentő nem ítéli sürgősnek = 1, a bejelentő sürgősnek ítéli = 2.

Az adatkezelés fontossága (súlya) a szervezet szempontjából: kritikus = 3, nem kritikus = 1.

A kockázati szint számértékét a tényezők összege adja.

Ha az adott eseménynél egy tényező nem értékelhető, akkor a legkisebb számértéket kell használni.

A tényezők alapján három kockázati szint használható:

Magas = 8 vagy több

Közepes = 5–7

Alacsony = 4

4.4. A „valószínűsíthetően magas kockázattal járó" adatkezelési műveletek megállapítása

Értékelési szempontok:

– Értékelés vagy pontozás: ideértve a profilalkotást és az előrejelzést is, különösen „az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők" alapján [GDPR rendelet (71) és (91) preambulum bekezdés]. Erre példaként említhető a pénzügyi vállalkozás, amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére, vagy a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat, vagy a vállalkozás, amely viselkedési vagy üzletszerzési profilokat készít a honlapjának használata vagy böngészése alapján.

– Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a „természetes személy tekintetében joghatással bíró" vagy „a természetes személyt hasonlóképpen jelentős mértékben érintő" döntések meghozatala [GDPR rendelet 35. cikk (3) bekezdés a) pontja]. Az adatkezelés adott esetben például egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. Az egyénekre nézve csekély vagy semmilyen hatással nem járó adatkezelés nem felel meg ennek a konkrét szempontnak. Az itt említett fogalmakról további felvilágosítást nyújt majd a 29. cikk szerinti adatvédelmi munkacsoport soron következő, profilalkotásról szóló iránymutatása.

– Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a „nyilvános helyek nagymértékű, módszeres megfigyelése" [GDPR rendelet 35. cikk (3) bekezdés c) pontja]. Az ilyen jellegű megfigyelés azért tartozik a figyelembe veendő szempontok közé, mivel a személyes adatok gyűjtése olyan körülmények között folyhat, ahol előfordulhat, hogy az érintettek nem tudják, ki gyűjti és hogyan használja fel adataikat. Ezen kívül az egyéneknek talán nincs lehetőségük elkerülni, hogy közterületeken (vagy nyilvános helyeken) érintetté váljanak ilyen adatkezelésben.

– Különleges adatok vagy fokozottan személyes jellegű adatok: ide tartoznak a személyes adatok a GDPR rendelet 9. cikkében meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a GDPR rendelet 10. cikkében meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok. Példaként említhető az általános kórház, amely nyilvántartást vezet a betegek kórtörténetéről, vagy a magánnyomozó, aki megőrzi az elkövetők adatait. A GDPR rendelet e rendelkezésein túlmenően bizonyos adatkategóriák tekinthetők úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ezek a személyes adatok (a fogalom általánosan ismert jelentését tekintve) különlegesnek minősülhetnek, mivel otthoni vagy magánjellegű tevékenységekhez kapcsolódnak (például elektronikus hírközlési tevékenységekhez, amelyek bizalmassága védendő), kihatnak valamely alapvető jog gyakorlására (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát), vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére (például pénzügyi adatok, amelyek csalásra használhatók). E tekintetben lényeges lehet, hogy az érintett vagy valamely harmadik személy már nyilvánosan hozzáférhetővé tette-e az adatokat. A személyes adatok nyilvános hozzáférhetősége az értékelés során egyik tényezőként figyelembe vehető, ha az adatok bizonyos célú további felhasználására lehet számítani. Ez a szempont olyan adatokra is vonatkozhat, mint például a személyes iratok, e-mailek, naplók, jegyzetelési funkcióval rendelkező e-olvasókból származó jegyzetek, valamint az életnaplózó alkalmazásokban tárolt, rendkívül személyes jellegű adatok.

– Nagy számban kezelt adatok: a GDPR rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a GDPR rendelet (91) preambulum bekezdés nyújt némi iránymutatást. Mindenesetre a GDPR rendelet 29. cikke szerinti adatvédelmi munkacsoport ajánlása szerint különösen az alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e:

a) az érintettek száma konkrét számadatként vagy a lakosság arányában;

b) a kezelt adatok mennyisége vagy adatfajták köre;

c) az adatkezelési tevékenység időtartama vagy állandó jellege;

d) az adatkezelési tevékenység földrajzi kiterjedése.

Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon.

– Adatkészletek egymással való megfeleltetése vagy összevonása

– Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok (GDPR rendelet 75. preambulum bekezdés): az ilyen jellegű adatok kezelése azért tartozik a figyelembe veendő szempontok közé, mivel nincs hatalmi egyensúly az érintettek és az adatkezelő között, ami azt jelenti, hogy az egyének adott esetben nem tudják adataik kezelését könnyen engedélyezni vagy ellenezni, illetve nem tudják a jogaikat gyakorolni. A kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek (ők úgy tekintendők, mint akik nem tudják tudatosan és átgondoltan ellenezni vagy engedélyezni adataik kezelését), a munkavállalók, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei (mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.), valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.

– Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében stb. A GDPR rendelet egyértelműen megfogalmazza [, hogy „a technológia elismert állásának megfelelő" módon meghatározott új technológia használata szükségessé teheti az adatvédelmi hatásvizsgálat elvégzését [GDPR rendelet 35. cikk (1) bekezdés, (89) és (91) preambulum bekezdés]. Ennek oka, hogy az ilyen technológiák használatához újfajta adatgyűjtési és -felhasználási formák kapcsolódhatnak, ami magas kockázattal járhat az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek. Az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat. Például bizonyos, a „dolgok internetét" használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését.

– Azok az esetek, amikor az adatkezelés önmagában véve „megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek" [GDPR rendelet 22. cikk és (91) preambulum bekezdés]. Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek. Erre példa, ha egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit, hogy eldöntse, kínál-e nekik hitelt.

Az esetek többségében az adatkezelő tekintheti úgy, hogy két szempontnak megfelelő adatkezelés esetében szükség van adatvédelmi hatásvizsgálatra.

4.5. A hatásvizsgálat mellőzésének esetei:

– ha az adatkezelés valószínűsíthetően nem jár „magas kockázattal [...] a természetes személyek jogaira és szabadságaira nézve" [GDPR rendelet 35. cikk (1) bekezdés];

– ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat. Ilyen esetekben felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei [GDPR rendelet 35. cikk (1) bekezdés];

– ha az adatkezelési műveleteket felügyeleti hatóság meghatározott, azóta változatlan feltételek mellett 2018. május előtt ellenőrizte (lásd a GDPR rendelet III. fejezet C. szakaszát);

– ha a GDPR rendelet 6. cikk (1) bekezdés c) vagy e) pontja szerinti adatkezelési művelet jogalappal rendelkezik az uniós vagy tagállami jogban, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat [GDPR rendelet 35. cikk (10) preambulum bekezdés], kivéve, ha a tagállam kimondta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni;

– ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) nem kötelező jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

5. A kockázatok kezelésére irányuló intézkedések:

Az azonosított kockázati tényezők kategorizálása után a következő lépés a kockázatokat csökkentő eljárások megfogalmazása, amelyek csökkentik vagy megszüntetik az adott kockázati tényezőt.

A kockázat kezelésére irányuló 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 adatbiztonság informatikai szempontú meghatározása.

6. Dokumentáció, azaz a kockázatelemzés összegzése, eredményének megállapítása:

Beszámoló elkészítése, a folyamat, a fennmaradó kockázatok leírása, gazdasági szempontú értékelése. Annak indoklással alátámasztott megállapítása, hogy szükséges-e az előzetes konzultáció.

7. Nyomon követés és felülvizsgálat:

Az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A kockázatok kezelésére hozott döntések rendszeres felülvizsgálatának a vezetési folyamat részévé kell válnia. Ezen túlmenően, az azonosítás–elemzés–értékelés–kezelésfolyamat (a kockázatok karaktereitől függő gyakoriságú) rendszeres ismétlése kritikus fontosságú az időbeli reagálás biztosítása miatt. A kockázatkezelési folyamatot magát, illetve eredményét (elemzés, döntéshozatal, ellenőrzés, kiegészítve a kontroll folyamatokkal) folyamatosan

dokumentálni kell, és gondoskodni kell a külső-belső érintettek megfelelő, rendszeres tájékoztatásáról is.