ADATKEZLÉSI- ÉS ADATVÉDELMI SZABÁLYZAT

FEHÉRVÁR MÉDIACENTRUM KFT.

Fehérvár Médiacentrum
ÚJSÁG · TELEVÍZIÓ · RÁDIÓ · ONLINE

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 közzététellel válik hatályossá.

Kelt: Székesfehérvár, 2021. június 30.

Hagymásy András
ügyvezető

Fehérvár Médiacentrum Kft. 1.
Adószám: 11837080-2-07
Bankszámlaszám: 12001008-01777122-00100004
8000 Székesfehérvár, Szent Vendel utca 17/A.

Tartalom

MELLÉKLETEK

17. sz. melléklet munkaszerződési kikötés

PREAMBULUM

(1) 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 irányelv 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.

(2) 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.

(3) 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.

(4) 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.

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

(6) 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.

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

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

(9) 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

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.

2. Értelmező rendelkezések

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

7. **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.

8. **adatkezelési nyilvántartás:** a GDPR 30. cikke alapján vezetett, személyesadat-kezeléseket tartalmazó nyilvántartás, amely az érintett adatkezeléshez kapcsolódó minden lényeges információt tartalmaz, jelen szabályzat **1. számú melléklete**.

9. **adatvédelmi incidens nyilvántartás:** a GDPR 33. cikk (5) bekezdése alapján vezetett nyilvántartás, amely jelen szabályzat **2. számú melléklete**.

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

11. **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.

II. RÉSZ

Adatvédelem felelősségi rendszere

3. Az adatkezelések szintjei

12. 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.

13. 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

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

15. 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.

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

17. 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

18. 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

19. 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.

20. Amennyiben a társaság alkalmazásában áll az adatvédelmi tisztviselő, munkaköri leírásában az adatvédelemmel kapcsolatos feladatokat rögzíteni kell.

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

22. 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) 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) éves jelentést tesz a személyes adatok kezelése, feldolgozása esetén a tájékoztatáshoz kapcsolódóan elutasított kérelmekről;
m) a társaság vezetője részére igény esetén éves jelentésben értékeli a társaság adatvédelmi tevékenységét;

n) adatvédelmi szempontból véleményezi a személyes adatokat tartalmazó informatikai nyilvántartásokra, szoftverekre vonatkozó fejlesztési javaslatokat;
o) feladat- és hatáskörében – a célhoz kötöttség elvére figyelemmel – jogosult a társaságnál folytatott adatkezelésekbe betekinteni, az adatkezelőtől felvilágosítást kérni;
p) ellenőrzi a GDPR-nak, valamint az egyéb uniós és tagállami adatvédelmi rendelkezéseknek, jelen belső szabályzatnak való megfelelést, képzést, auditokat;
q) közreműködik a betekintési és hozzáférési jogosultságok felügyeletében;
r) szakmai tanácsot ad a hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését.
s) 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

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

24. A társaság valamennyi adatkezelése vonatkozásában a személyes adatok 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.

25. Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét, jogaik gyakorlásának lehetőségét. A társaság a személyes adatok kezelésére vonatkozóan titoktartási kötelezettséget ír elő, amelyet a **17. sz. melléklet** tartalmaz.

26. A személyes adatokhoz való hozzáférést a társaság, elektronikus úton (hálózati meghajtó, beléptető rendszer) jogosultsági szintek megadásával korlátozza.

27. 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.

28. 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 a személyes adatok magasabb szintű védelmét biztosítja.

29. 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.

30. A társaság személyes adatok automatizált feldolgozását végzi. Az automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja:

a) az érintett tájékoztatását;
b) az eszköz pontosságát, rendeltetésszerű működését;
c) a jogosulatlan adatbevitel megakadályozását;
d) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
e) annak ellenőrizhetőségét és megállapíthatóságát, ha a személyes adatokat adatátviteli berendezés alkalmazásával továbbították vagy továbbíthatják;
f) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
g) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát;
h) az automatizált feldolgozás során fellépő hibákról jelentés készítését;
i) az érintettnek biztosítani kell az emberi beavatkozás lehetőségét, lehetővé kell tenni, hogy álláspontját kifejthesse, és a döntéssel szembeni kifogást közölje.

8. Az adatvédelem alapvető szabályai

31. A személyes adatok kezelésének helyszínéül szolgáló épület megfelelő fizikai, és tűzvédelméről gondoskodni kell. A személyes adatok kezelése zárható helyiségébe csak az arra jogosultak léphetnek be.

32. A társaság indokolt esetben külön adatbiztonsági szabályzatot alkalmaz.

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

34. A nem irodai dolgozó (pl. takarító, karbantartó) személyes adatokkal 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.

35. Az társaság az informatikai rendszerek frissítéséről az adott szoftver fejlesztője által meghatározott rendszerességgel gondoskodik, tesztelését nem valós adatokkal végezheti. Az informatikus programok telepítését, frissítését megelőzően, megfelelő időben értesíti a társaságot, annak érdekében, hogy a személyes adatokhoz való hozzáférés folyamatosan biztosított legyen.

36. A társaság azon munkavállalói, akik személyes adat meghatározott csoportját nem kezelik (pl. alkalmazotti adatok, alkalmazottak pénzügyi adatai, ügyféladatok) azokhoz nem férhetnek hozzá.

37. A rendszergazdai jogosultsággal rendelkezők esetén is nyomon követhetővé teszi azt, hogy személyhez rendelhető legyen valamennyi adatkezelési művelet (pl. admin1, admin2, admin3 felhasználónévvel).

38. A társaság elektronikus adatfeldolgozásra, nyilvántartásra alkalmazott szoftvere lehetővé teszi a rendszer naplózhatóságát, hogy azonosítható legyen, mely felhasználó, mikor, mit rögzített, vagy törölt. A társaság, csak eredeti 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.

40. A társaság gondoskodik mind az elektronikus, mind a papír alapú bejövő és kimenő kommunikáció ellenőrzéséről, vírusmentesítéséről. Egészségügyi adat elektronikusan kizárólag adathordozón, vagy titkosított csatornán, illetve jelszavas védelemmel továbbítható.

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 a személyes adatokat tartalmazó dokumentumokat. Közösen használt nyomtató esetén biztosítani kell, hogy a nyomtatni kívánt dokumentum, a nyomtató személy jelenlétében jelenjen meg.

43. A személyes adatot 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 rendszerekbe megfelelő azonosítás, hitelesítést követően lehet hozzáférni.

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

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

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

48. A társaság felhőszolgáltatás igénybe vétele esetén olyan szolgáltatót választ, amelynek tárhelye az Európai Unió valamely országában található.

49. A tárasaság eszközein a felhasználónevek, jelszavak megjegyzése nem állítható be. Jelszó papír alapon nem tárolható.

50. Személyes adatot tartalmazó papír alapú dokumentumot a társaság épületéből kivinni, az 1. sz. mellékletben megjelölt helyről más helyre áthelyezni, csak vezetői engedéllyel lehet. Az irat mozgás dokumentálása érdekében a **9. sz. mellékletet** kell kitölteni.

9. A társaság adatkezelési tájékoztatója

51. A Társaság általános adatkezelési tájékoztatóját a **3. sz. melléklet** tartalmazza.

52. Amennyiben a társaság eseti adatkezelést végez (pl. rendezvény szervezése, álláshirdetés) úgy a vonatkozó tájékoztató kidolgozásáról és az érintettek részére elérhetővé tételéről megfelelően gondoskodik. A társaság az eseti adatkezelést megelőzően az adatvédelmi tisztviselő véleményét beszerzi.

IV. RÉSZ
AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI

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

10. Az érintett hozzájárulása

54. Amennyiben a személyes adatok kezelése hozzájáruláson alapul, az érintett hozzájárulását az **4. számú melléklet** szerinti adatkérő lap szerinti tájékoztatással és tartalommal kell beszerezni. A hozzájárulás önkéntességét biztosítani kell

55. 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.

56. 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 meg kell adni.

57. 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.

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

59. 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.

60. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a rá vonatkozó jogi kötelezettség teljesítése céljából, törvény eltérő rendelkezésének hiányában további külön hozzájárulás nélkül, valamint a hozzájárulás visszavonását követően is kezelheti.

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

11. Szerződés, mint jogalap

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

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

64. A szerződésekben külön adatvédelmi záradékot kell feltüntetni, amiben rögzíteni kell a papír alapú, illetve az elektronikus védelmi intézkedéseket a szerződésben szereplő személyes adatok védelme érdekében.

65. 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.

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

12. Jogi kötelezettség teljesítése

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

68. 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

69. Személyes adat kezelhető abban az esetben is, amennyiben az adatkezelő, vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

70. Amennyiben a társaság jogos érdeke alapján kíván adatot kezelni, úgy előzetesen érdekmérlegelési tesztben szükséges felmérni az adatkezelés jogszerűségét az **5. számú melléklet** alapján.

71. Ügyféladatok, alkalmazotti adatok további kezelésére ezen a jogalapon sor kerülhet, azonban meg kell vizsgálni ezen jogcímen alapuló adatkezelést megelőzően, hogy az érintett a személyes adatok gyűjtésének időpontjában számíthat-e ésszerűen arra, hogy adatkezelésre adott célból kerülhet sor.

72. Személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.

14. Személyes adatok gyűjtési céltól eltérő kezelése

73. Személyes adatok gyűjtési céljuktól eltérő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljával. A további adatkezelés megkezdése előtt indokolt kikérni az adatvédelmi tisztviselő állásfoglalását.

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

V. RÉSZ

MUNKAVISZONNYAL KAPCSOLATOS ADATKEZELÉSEK

15. Személyügyi nyilvántartás

75. 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.).

76. A munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyiségi jogát nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

77. A társaság köteles a munkavállalót tájékoztatni személyes adatainak kezeléséről. A társaság a munkavállalóra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy a munkavállaló hozzájárulásával közölhet.

78. A munkaviszonyból származó kötelezettségek teljesítése céljából a társaság a munkavállaló személyes adatait - az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint - adatfeldolgozó számára átadhatja. Erről a munkavállalót előzetesen tájékoztatni kell.

79. A társaság a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A társaság ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. A társaság előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak.

80. Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a Munka törvénykönyvén és a munkáltató jogos érdekeinek érvényesítésén alapul.

81. A társaság alkalmazottak **7. sz. mellékletben** továbbá a hatályos jogszabályokban meghatározott adatait, az ott meghatározott jogalap szerint és célból kezeli. A társaság az alkalmazotti adatokat törzslapon tartja nyilván.

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

83. 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.

84. 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.

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

86. 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.

87. A társaság a munkaszerződés megkötésével egyidejűleg a jelen szabályzat **7. számú melléklete** szerinti Tájékoztató átadásával tájékoztatja a munkavállalót személyes adatainak kezeléséről és a személyhez fűződő jogokról.

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

89. A társaság által kiírt álláspályázatokra beküldött jelentkezésekhez mellékelni kell a pályázóknak a személyes adatok kezeléséhez a pályázati anyaggal együtt megadott személyes hozzájárulását. A pályázat elbírálása után az eredménytelen pályázók személyes adatait tartalmazó adathordozókat a pályázónak – kérésére – indokolatlan késedelem nélkül, de legkésőbb 1 hónapon belül vissza kell küldeni, vagy a pályázónak a személyes adatai további pályázatok során történő felhasználására vonatkozó hozzájárulása hiányában meg kell semmisíteni. A megsemmisítésről (törlésről) jegyzőkönyvet kell felvenni.

90. A társasághoz bármilyen formában álláskeresési céllal (hirdetésre, spontán módon) eljuttatott önéletrajzokban lévő személyes adatok kezeléséhez az érintett hozzájárulását kell kérni tárolás céljára. Alkalmazás hiányában a személyes adatokat törölni kell.

91. A társaság foglalkoztatottjai kötelesek a feladatkörükben tudomásukra jutott személyes adatokat, üzleti, szakmai titkokat, szellemi termékeket, ügyintézéshez kapcsolódó más érzékeny információkat megőrizni a törvény, illetve a **13. mellékletben** foglaltak szerint.

92. A szenzitív adatok körébe tartozó információk kezelése során fokozott körültekintéssel kell eljárni.

93. A jogviszonyból származó kötelezettségek teljesítése céljából a társaság az alkalmazott személyes adatait - az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint – közös adatkezelő, illetve adatfeldolgozó számára átadhatja. Erről az alkalmazottat előzetesen tájékoztatni kell.

94. Az alkalmazottat csak a jogviszonnyal összefüggő magatartása körében ellenőrizheti. A társaság ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak

az emberi méltóság megsértésével. Az alkalmazott magánélete nem ellenőrizhető. A társaság előzetesen tájékoztatja az alkalmazottat azoknak a technikai eszközöknek az alkalmazásáról, amelyek az alkalmazott ellenőrzésére szolgálnak.

95. A társaság nem jogosult az alkalmazotti okmányainak másolására, amennyiben erre jogszabály nem hatalmazza fel. Erre való tekintettel az okmányazonosító rögzítésére a személyi ügyekkel foglalkozó alkalmazott jogosult, amely rögzítés helyességét a vezetője igazolja.

96. A személyi anyagba csak az arra jogosultak tekinthetnek be, amelynek biztosítására betekintési naplót kell vezetni.

16. Alkalmassági vizsgálatokra vonatkozó adatkezelés

97. 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.

98. A munkaalkalmasságra, felkészültségre irányuló tesztlapokat a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal.

99. 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.

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

101. 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 **8. számú melléklete** tartalmazza.

102. 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.

103. 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.

104. 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

105. 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.

106. A személyes adatok a munkaviszony megszűnését követő 50 évig kezelhetőek. A teszteket, és a munkavállalókra vonatkozó értékeléseket a személyi anyagtól elkülönítve kell, elzártan tárolni.

17. Önéletrajzok kezelése

107. Annak érdekében, hogy a nem pályázati kiírás eredményeként érkező önéletrajz benyújtója, illetve a pályázat keretében benyújtott önéletrajzok további tárolása érdekében személyes adatok védelméhez fűződő joga ne sérüljön, a társaság honlapján az önéletrajzok kezelésével és tárolásával kapcsolatos tájékoztatót kell elhelyezni az Kapcsolat link alatt, melyben fel kell hívni a figyelmet arra, hogy az érintettnek a beküldött önéletrajzához csatolnia kell egy nyilatkozatot, amelyben hozzájárul önéletrajzának 3 hónapig tartó kezeléséhez. Amennyiben a beérkezett nyilatkozat a hozzájárulást nem tartalmazza, a társaság kizárólag annak vizsgálatára jogosult, hogy a pályázati anyagnak megfelelő betöltetlen álláshellyel rendelkezik-e, amennyiben ilyen álláshely nem áll rendelkezésre, az anyagot a benyújtójának vissza kell küldeni vagy meg kell semmisíteni.

108. Az önéletrajz tárolási céllal legfeljebb egy évig történő megőrzéséhez az érintett hozzájárulását adhatja a **4. számú melléklet** szerint.

109. Az állásfelhívás feladása során jelezni kell, hogy az önéletrajzok tárolási ideje az adott pályázat elbírálása, amennyiben a jelentkezés pályázattól függetlenül érkezett, a jelentkezés benyújtásától számított 3 hónap. A fel nem vett személyek önéletrajza a felvett, azonban próbaidő alatt megüresedő munkakör betöltése céljából kezelhető, amennyiben ehhez az érintett hozzájárul.

110. Az adattárolási határidő lejártát, vagy az érintett hozzájárulásának visszavonását követően a pályázati anyagokat meg kell semmisíteni, ha arra a jelentkező külön igényt tart, részére vissza kell küldeni.

111. A kezelhető személyes adatok köre, a természetes személy neve, születési ideje, helye, anyja neve, lakcím, képesítési adatok, fénykép, telefonszám, e-mail cím, korábbi munkáltatói értékelés (ha van).

112. A személyes adatok kezelésének célja, a megfelelő munkaerő kiválasztása. Az érintettet tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra.

113. Az adatkezelés jogalapja pályázati kiírás esetén az adatkezelő jogos érdeke, tárolás esetén a hozzájárulás, felvett személyek esetén a szerződés.

114. Az önéletrajzokat a társaságnál munkáltatói jogok gyakorlására jogosult vezető, személyügyi feladatokat ellátó munkavállalók kezelhetik.

115. Amennyiben a társaság képviselője az állásinterjú során jegyzetet vesz fel, előzetesen az érintett hozzájárulását kell kérni és a végén számára lehetővé kell tenni a jegyzet megismerését, amelyhez észrevételt tehet. Az állásinterjú végén az érintett amennyiben a jegyzet tartalmával egyet ért, azt aláírja, aláírás megtagadása esetén a jegyzetet meg kell semmisíteni.

116. Az álláspályázathoz kapcsolódóan a társaság nem jogosult korábbi munkáltatók megkeresésére.

117. A társaság a pályázó nyilvánosan közzétett, közösségi oldalakon szereplő adatait ellenőrizheti (azonban nem tárolhatja), amelynek tényére a pályázat kiírásakor, illetve a honlapon felhívja a figyelmet. A társaság a pályázó közösségi oldal zárt csoporthoz kapcsolódó tevékenységet nem ellenőrizhet.

118. A társaság anonim álláshirdetést abban az esetben adhat fel, ha profilbővítésként a konkurencia elől rejtve kíván maradni, illetve ha meglévő dolgozója helyett megfelelőbb munkaerőt kíván kiválasztani.

119. A társaság a munkaerő kiválasztása során előzetes tájékoztatást követően jogosult a jelentkező közösségi oldalon közzétett profiloldalának megtekintésére és a munkakör betöltéséhez szükséges adatok kezelésére. A társaság a pályázó közösségi oldal zárt csoporthoz kapcsolódó tevékenységet nem ellenőrizhet.

120. A 118/2001. (VI. 30.) Korm. rendelet 10. § (1) bekezdés e) pontja meghatározza, hogy milyen adatokat nem lehet kezelni magán-munkaközvetítés során. A jogszabály értelmében tilos olyan személyes adatokat kezelni, amelyekre a munkát keresők alkalmasságának a megítéléséhez nincs szükség, illetve amelyek a keresett munkával nincsenek közvetlen összefüggésben.

121. Az álláspályázat részenként hatósági erkölcsi bizonyítvány kérhető, amennyiben erre jogszabály lehetőséget ad, továbbá ha a munkakör jelentős vagyoni érdek védelméhez, törvény által védett titok megőrzéséhez, veszélyes áru kezeléséhez kapcsolódik.

18. Elektronikus levelezőrendszer ellenőrzéséhez kapcsolódó adatkezelés

122. A társaság munkavállalóit azért ellenőrizheti, hogy megbizonyosodjon róla, hogy üzleti, személyes adatokra vonatkozó titoktartási kötelezettségüknek eleget tesznek,

munkaköri feladatuk ellátásáról, azok minőségéről, a munkavállalók, készségéről, képességéről meggyőződjön.

123. A társaság e-mail fiókot bocsát a munkavállaló rendelkezésérem, amely e-mail címet és fiókot a munkavállaló a munkaköri feladatai céljára használhatja, abból a célból, hogy a munkavállalók egymással kapcsolatot tartsanak, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel. A munkavállaló az elektronikus levelezőrendszert magán célra nem használhatja, a fiókban személyes leveleket nem kezelhet, amely tilalomra a társaság félévente emlékezteti alkalmazottjait.

124. Az ellenőrzés jogalapja a munkáltató jogos érdeke, célja, a munkaviszonyra vonatkozó kötelezettségek megtartásának ellenőrzése, a megfelelő munkavégzés biztosítása.

125. A társaság elektronikus levelezőrendszerének informatikai védelméről, így annak rendelkezésre állásáról, sértetlenségéről, bizalmasságáról a rendszergazda útján gondoskodik. A levelezés biztonsági mentéséről a tárhelyet biztosító szerver biztonsági mentésével azonos időközönként gondoskodik, amelynek hiányában havi rendszerességű biztonsági mentés készül.

126. Az elektronikus levelezőrendszer használata során az érintett munkavállaló köteles megfelelő körültekintéssel eljárni, mind a címzettek megadása, titkos másolatok alkalmazása, mind a dokumentumok csatolása során. Ügyelni kell arra, hogy a címzettek és másolatot kapó személyhez kapcsolódó elektronikus levelezési cím is személyes adat.

127. Az elektronikus levelezés során törekedni kell a személyes adatok titkosítására. A dokumentumok tervezeteit személyes adatok feltüntetése nélkül kell egyeztetésre küldeni.

128. A munkahelyi levelezőrendszer használata kizárólag munkahelyi eszközökön engedélyezett.

129. A munkáltató jogosult az e-mail fiók tartalmát és használatát rendszeresen – 3 havonta – ellenőrizni. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek teljesítésének ellenőrzése, jogalapja a munkáltató jogos érdeke.

130. Az ellenőrzésre és adatkezelésre a munkáltató vezetője, vagy a munkáltatói jogok gyakorlója jogosult.

131. Lehetőség szerint biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során, távollétében két személy jelenlétében jegyzőkönyvet kell felvenni a tapasztaltakról

132. Az ellenőrzés megkezdése előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről, ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az ellenőrzés eredményével kapcsolatban.

133. Az ellenőrzés során a fokozatosság elvét kell érvényesíteni, így elsődlegesen levél címéből és tárgyából kell következtetést levonni arra vonatkozóan, hogy az a munkavállaló munkaköri feladatával kapcsolatos, és nem személyes célú. A nem személyes célú e-mailek tartalmát a társaság korlátozás nélkül vizsgálhatja.

134. Amennyiben megállapítható, hogy a munkavállaló az elektronikus levelezőrendszert személyes célra használta, fel kell szólítani, hogy a személyes adatokat haladéktalanul törölje. A munkavállaló távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli.

135. Az elektronikus levelező rendszer jelen szabályzatba ütköző használata miatt a társaság a munkavállalóval szemben, az Mt. 56. § alapján, a munkaszerződésben rögzített jogkövetkezményeket alkalmazhat.

136. A munkavállaló az elektronikus levelezőrendszer ellenőrzésével együtt járó adatkezeléssel kapcsolatban jelen szabályzatnak az érintett jogairól szóló részében írt jogokat gyakorolhatják.

137. A jogviszony megszűnését megelőzően a munkavállaló gondoskodik arról, hogy az esetleges magáncélú leveleit törölje. A jogviszony megszűnését követően a társaság az elektronikus levelezőrendszerben tárolt személyes adatokat megsemmisíti.

138. Az alkalmazott munkahelyi levelezőrendszer GDPR-nak való megfelelősségére vonatkozó hatásvizsgálat eredményét a társaság a szoftverfejlesztőtől beszerzi.

139. Az a munkavállaló, aki a levelezőrendszer működésében rendellenességet észlel, vagy olyan személyes adat válik számára hozzáférhetővé, amelynek megismerésére nem jogosult, köteles azonnal jelezni a rendszergazda, és a társaság vezetője felé.

140. A társaság a 2018. május 25. napját követően bevezetésre, vagy módosításra kerülő ellenőrzési eljárás, alkalmazott szoftver esetén hatásvizsgálatot végez, az alkalmazott szoftver GDPR-nak megfelelésére vonatkozó igazolást beszerzi.

19. Az informatikai eszközök ellenőrzésével kapcsolatos adatkezelés

141. A társaság jelen szabályzattal előírja, hogy az általa biztosított számítástechnikai vagy elektronikus eszközt így különösen számítógépet, laptopot, tabletet a munkavállaló kizárólag a munkavégzéshez használhatja, ezek magáncélú használatát a társaság megtiltja, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem kezelhet és nem tárolhat.

142. Az elektronikai eszközök időszakos – félévente – szerverre történő mentéséről gondoskodni kell, megelőzően az érintetteket fel kell hívni, hogy esetleges személyes adataikat távolítsák el az adathordozókról.

143. A társaság által biztosított mobil adathordozókon kívül egyéb eszköz nem csatlakoztatható a társaság informatikai eszközeihez, jelszavas védelmi ellenőrzéssel biztosítani kell az idegen eszközök használatának kizárását.

144. Az informatikai eszköz javítására a társaság rendszergazdája intézkedik, amennyiben ő nem tudja megjavítani, úgy a javítás idején jelen kell lennie, hogy személyes adat jogosulatlanul ne kerülhessen ki az informatikai eszköz adathordozójáról. A harmadik személy által végzett javítás idején akkor lehet az informatikus távol, ha adathordozót (winchestert) nem ad át, vagy a harmadik személy igazolja, hogy az általa folytatott tevékenység a GDPR rendeletnek megfelel, és titoktartási nyilatkozatot tesz.

145. Az informatikai eszköz selejtezését, értékesítését megelőzően gondoskodni kell az adathordozó fizikai megsemmisítéséről.

146. A jogviszony megszűnését megelőzően a munkavállaló gondoskodik arról, hogy az esetlegesen informatikai eszközön lévő magáncélú adatait törölje. A jogviszony megszűnését követően a társaság az informatikai eszközön tárolt személyes adatokat megsemmisíti.

147. A munkáltató az informatikai eszközökön tárolt adatokat ellenőrizheti. Az informatikai eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben a 18. cím rendelkezései irányadók.

148. A munkavállaló köteles 24 órán belül bejelenteni a társaság vezetője részére, ha informatikai eszközét elvesztette és közölni, hogy az eszközön megközelítőleg hány, és milyen jellegű személyes adat volt.

149. A távmukavégzés a társaság által rendelkezésre bocsátott informatikai eszköz felhasználásával engedélyezhető. A távmunkavégzés esetén a munkavállalót tájékoztatni kell a társaság általi ellenőrzés és az informatikai eszköz használata korlátozásának 18. címben és jelen címben foglalt szabályairól, továbbá arról a szervezeti egységről, amelyhez a munkavállaló munkája kapcsolódik.

150. Az informatikai eszközök védelméről a rendszergazda gondoskodik, amelynek során megfelelő intézkedéseket tesz annak érdekében, hogy az eszköz elvesztése esetén a tárolt személyes adatokhoz ne lehessen hozzáférni.

20. A munkahelyi internethasználat ellenőrzésére vonatkozó adatkezelés

151. A munkavállaló csak a munkaköri feladatával összefüggő honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja.

152. A társaság informatikai eszközeire interneten elérhető szoftver csak rendszergazdai engedéllyel telepíthető. A rendszergazda a szoftver telepítését személyesen, vagy távoli hozzáféréssel történő rendszergazdai felhasználónév és jelszó megadása után engedélyezi. A külső forrásból kapott vagy letöltött, nem engedélyezett programok használata tiltott!

153. A fájl letöltő-, játék-, csevegő-, szexuális szolgáltatásokat kínáló oldalak látogatása szigorúan tilos.

154. A munkaköri feladatként a társaság nevében elvégzett internetes regisztrációk jogosultja a társaság. A személyes adatok megadása is szükséges a regisztrációhoz, a munkaviszony megszűnésekor azok törlését kezdeményezi a társaság. A társaság informatikai eszközein nem megengedett a felhasználónév, jelszó megjegyzésének engedélyezése. A társaság nem jogosult megismerni a munkavállaló által alkalmazott jelszót.

155. A munkavállaló munkahelyi internethasználatát a társaság 18. cím rendelkezései szerint ellenőrizheti és az ott meghatározott jogkövetkezményeket alkalmazhatja.

21. A céges mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

156. A társaság a céges mobiltelefon magáncélú használatát nem engedélyezi, az csak munkavégzéssel összefüggő célokra használható, és a társaság valamennyi kimenő hívószámot és adatokat, továbbá a mobiltelefonon tárolt adatokat ellenőrizheti.

157. A munkavállaló köteles bejelenteni a társaságnak, ha a céges mobiltelefont magáncélra használta. A munkáltató jogosult nyilatkoztatni a munkavállalót, amennyiben más azonos munkakört betöltő munkavállalói átlaghoz képest több, mint 50%-al magasabb telefonszámla keletkezik adott munkavállaló esetén. Ilyen esetben a társaság a telefonszolgáltatótól bekéri a hívásadatok részleteit és felhívja a munkavállalót arra, hogy a magáncélból hívott számokat tegye felismerhetetlenné. A társaság a magáncélú hívások költségeinek megfizetésére a munkavállalót kötelezheti.

158. A munkavállaló jogviszonyának megszűnését megelőzően gondoskodik arról, hogy az esetleges magáncélú telefonszámait törölje. A jogviszony megszűnését követően a társaság a mobiltelefonon tárolt személyes adatokat megsemmisíti.

159. A munkavállaló köteles 24 órán belül bejelenteni a társaság vezetője részére, ha céges mobiltelefonját elvesztette.

160. A céges mobiltelefonokat el kell látni olyan programmal, amely lehetővé teszi a képernyő zárolását, illetve a telefonon, valamint a SIM kártyán tárolt adatok törlését abban az esetben, ha illetéktelen személy kívánna hozzáférni a telefonon tárolt személyes adatokhoz.

161. Az ellenőrzésre és jogkövetkezményire a 18. cím rendelkezései irányadók.

22. A navigációs rendszer alkalmazásával kapcsolatos adatkezelés

162. A navigációs rendszer (GPS) alkalmazásának jogalapja a munkáltató jogos érdeke, célja a munkafolyamatok hatékony megszervezése, logisztika, a munkáltató üzleti érdekeinek, illetve a munkavállalók életének, testi épségének, a gépjárműnek és a rakománynak védelme, elektronikus menetlevél elkészítése.

163. A kezelt adatok a gépjármű rendszáma, a megtett útvonal, távolság, idő, tartózkodási hely, gépjárműhasználat ideje, amely adatok részben a gépjárművezető személyes adatának is minősülnek.

164. Ellenőrzésre kizárólag munkaidőben kerülhet sor, a munkavállalók földrajzi helyzete munkaidőn kívül nem ellenőrizhető. Egyebekben az ellenőrzésre és jogkövetkezményire a 19. cím rendelkezései irányadók, azzal, hogy a munkáltató jogosult nyilatkoztatni a munkavállalót, amennyiben a menetlevélben szereplő helyek közti távolságok az útvonaltervező programhoz képest 20%-al nagyobb eltérést mutatnak, amely esetben a költség megtérítésére kötelezheti a munkavállalót.

165. Amennyiben a gépjárművet a munkavállaló magáncélra is használhatja, ellenőrzése nem lehetséges.

166. Az alkalmazott navigációs rendszer GDPR-nak való megfelelősségére vonatkozó hatásvizsgálat eredményét a társaság beszerzi.

23. A munkahelyi be- és kiléptetéssel kapcsolatos adatkezelés

167. A beléptető rendszer alkalmazása esetén tájékoztatást kell elhelyezni az adatkezelő személyéről és az adatok kezelésének módjáról.

168. A munkaköri leírásban meghatározott munkaidőt követően, a társaság vezetőjének engedélye hiányában a munkahelyen jogszerűen nem lehet tartózkodni.

169. A kezelhető személyes adatok köre, a természetes személy neve, belépés, kilépés ideje. Az adatkezelés jogalapja, a munkáltató objektumának megfelelő használatához, munkavállalók megfelelő, biztonságos munkavégzéséhez fűződő jogos érdekeinek érvényesítése.

170. A személyes adatok kezelésének célja, a munkavállalói kötelezettségek teljesítésének ellenőrzése.

171. Az adatok a társaságnál munkáltatói jogok gyakorlására jogosult vezető, adatfeldolgozóként a társaság vagyonvédelmi megbízottjának foglalkoztatottjai részére hozzáférhetők, továbbíthatók.

172. A személyes adatok kezelésének időtartama, 3 év.

173. A beléptető rendszer alkalmazása esetén meg kell határozni, hogy a beléptető eszköz, mely munkavállalóhoz tartozik. Rögzíteni kell a belépési jogosultsági kört az adott eszköz kapcsán. A beléptető eszközön személyes adat nem lehet feltüntetve.

174. Az elektronikus beléptető eszköz elvesztése esetén az 24 órán belül jelezni kell az ügyvezető vezető részére és gondoskodni kell az eszköz tiltásáról.

175. Biometrikus azonosítóra épülő beléptetésre akkor van lehetőség, adat és információbiztonsági szabályok megtartása, minősített, különleges, vagy törvény által védett adat védelme, a munkáltató jelentős vagyoni érdeke, lőfegyver, lőszer, robbanóanyag, vagy mérgező, veszélyes vegyi, biológiai, nukleáris anyag tárolása miatt a munkavállaló kétséget kizáró azonosítása miatt szükséges.

176. A munkavállaló biometrikus adatának tárolására csak biometrikus sablon alkalmazását követően kerülhet sor, amely alapján a biometrikus adat ismételt előállítása, visszafejtése nem lehetséges.

177. Az alkalmazott elektronikus beléptető rendszer GDPR-nak való megfelelősségére vonatkozó hatásvizsgálat eredményét a társaság beszerzi.

24. A munkahelyi kamerás megfigyelésre vonatkozó adatkezelés

178. A társaság a székhelyén, telephelyén, az ügyfélfogadásra nyitva álló helyiségeiben az emberi élet, testi épség, veszélyes anyag, az üzleti titok védelme, baleset körülményeinek tisztázása, káresemény kivizsgálása és a vagyonvédelem céljából elektronikus megfigyelőrendszert alkalmaz, amely képrögzítést és tárolást is lehetővé tesz, ez alapján személyes adatnak tekinthető az érintett magatartása is, amit a kamera rögzít. Meghatározott vagyontárgy védelme esetén a kamerának közvetlenül és kizárólagosan a védendő vagyontárgyra kell irányulnia.

179. Az adatkezelés jogalapja a munkáltató és a megbízottként eljáró személyek megbízóinak jogos érdekeinek érvényesítése, továbbá figyelembe vettük a kamerafelvételen nem szereplő sértett jogos érdekét.

180. A megfigyelőrendszer adott területen történő alkalmazásának tényéről a megfigyelt területre való belépést megelőzően, jól látható helyen, jól olvashatóan, az érintettek tájékozódását elősegítő módon figyelemfelhívó jelzést, tájékoztatást kell elhelyezni. A tájékoztatást minden egyes kamera esetén biztosítani kell. A tájékoztatás mintát a **10. számú melléklet** tartalmazza.

181. Nem alkalmazható elektronikus megfigyelőrendszer vagy technikai ellenőrzésre szolgáló más eszköz olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, mosdóban, illemhelyen, egészségügyi vagy pszichológiai vizsgálat céljára szolgáló helyiségben, ideértve a vizsgálati helyiséghez tartozó váróhelyiséget is, étkezőben, munkahelyi pihenésre szolgáló helyiségben. A megfigyelőrendszer közterületre nem irányulhat.

182. Technikai ellenőrzéssel összefüggően sem helyezhető el a munkavégzés, munkahelyi viselkedés megfigyelése céljából kamera olyan helyiségekben, ahol állandó munkavégzés folyik, sem pedig a munkaközi pihenés céljául szolgáló helyiségekben, kijelölt dohányzóhelyen, ügyeleti helyiségben.

183. A fenti rendelkezések alól kivételt képeznek az olyan munkahelyiségek, ahol a munkavállalók élete, testi épsége veszélyben lehet, így pl. kivételesen működtethető

kamera szerelőcsarnokban vagy más veszélyforrást tartalmazó objektumban, helyiségben.

184. A rögzített felvételek felhasználás hiányában maximum 3 (három) munkanapig őrizhetők meg. Felhasználásnak az minősül, ha a rögzített képfelvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként kívánják felhasználni. Akinek a felvételen szerepel három munkanapon belül kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Amennyiben a felvétel kimentésére vonatkozó igény benyújtására kerül sor, haladéktalanul intézkedni kell a felvétel kimentéséről és elkülönített, biztonságos tárolásáról.

185. A jelentős értéket képező eszközök, áruk elhelyezéséül szolgáló helyiségeiben, így különösen garázsban, egyéb, jelentős értéket képviselő eszközök tárolására szolgáló raktárban és az azokhoz vezető folyosókon elhelyezhető és működtethető kamera, azok működéséről azonban jól látható helyen és módon tájékoztatni kell az érintetteket.

186. Ha a munkahely területén jogszerűen senki sem tartózkodhat - így különösen munkaidőn kívül vagy a munkaszüneti napokon - akkor a munkahely teljes területe (így például az öltözők, illemhelyek, munkaközi szünetre kijelölt helyiségek) megfigyelhető.

187. A kamerák által vett képet közvetítő berendezést úgy kell elhelyezni, hogy azt csak az a személy láthassa, akinek a kamera által közvetített kép figyelése a munkaköri feladatainak részét képezi. A rögzített adatok megtekintésére a jogsértések feltárása és a rendszer működésének ellenőrzése céljából a kezelő személyzet, a társaság vezetője és helyettese, továbbá a megfigyelt terület munkahelyi vezetője jogosult.

188. A megfigyelés és a tárolt képfelvételek visszanézése kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából végezhető.

189. A kamerák által közvetített képet az adattároló egységen kívül más eszközzel rögzíteni nem lehet.

190. Az adattároló eszközt elzárt helyen kell őrizni. A tárolt képfelvételekhez való hozzáférésnél az adatkezelő személyének azonosíthatónak kell maradnia. A képfelvételek visszanézését és a képfelvételekről készített mentést dokumentálni kell.

191. A jogosultság indokának megszűnését követően a tárolt képfelvételekhez való hozzáférést haladéktalanul meg kell szüntetni. A rögzítő készülékben elkülönített merevlemezről fut az operációs rendszer és a tárolt felvételek. A felvételekről külön biztonsági másolat nem készül, távolról nem hozzáférhető.

192. A jogsértő cselekmény észlelését követően a cselekményről készült felvétel rögzítéséről és a szükséges eljárás kezdeményezése felől intézkedni kell, egyben tájékoztatni kell az eljárásra jogosult szervet, hogy a cselekményről képfelvétel készült.

193. A tárolt képfelvételek átadását megelőzően meg kell győződni arról, hogy ki nem adható adatok ne szerepeljenek, harmadik személyek személyhez fűződő joga ne

sérüljön. Az át nem adható adatokat anonimizálni szükséges (pl. rendszámok, harmadik személyek).

194. Az alkalmazott megfigyelő rendszer GDPR-nak való megfelelősségére vonatkozó hatásvizsgálat eredményét a társaság beszerzi, a 2018. május 25. napján követően alkalmazásra kerülő, munkavállalók, illetve ügyfelek megfigyelésére alkalmas kamera alkalmazása esetén a társaság indokolt esetben hatásvizsgálatot végez.

25. A tanulmányi szerződésekre vonatkozó adatkezelés

195. A társaság a munkavállalóval tanulmányi szerződést köthet, az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződésen alapul, amely tájékoztatás történhet a szerződésben is.

196. Az adatkezelés jogalapja a szerződés, adatkezelési idő a jogviszony megszűnését követő 5 év.

197. Az érintettet személyes adatai a képzést végző oktatási intézmény, mint közös adatkezelő részére átadhatók, amelyről a szerződésben tájékoztatni kell az érintettet.

198. A munkavállalóval kötött szerződéshez kapcsolódó adatkezelési tájékoztató szövegét a **11. számú melléklet** tartalmazza.

199. A személyes adatokat, a társaság személyügyi feladatait ellátó munkavállalói és adatfeldolgozói kezelhetik.

200. A tanulmányi szerződés megkötésénél az Mt. 229. § (1) bekezdése és a törvény további rendelkezéseit is figyelembe kell venni.

VII. RÉSZ

HOZZÁJÁRULÁS, MINT AZ ADATKEZELÉS JOGALAPJA

26. A honlap böngészésre vonatkozó (cookie) adatkezelés

201. A cookie (süti) egy olyan adat, amit a meglátogatott weboldal küld a látogató böngészőjének, hogy az eltárolja és később betölthesse a tartalmát.

202. Az adatkezelés jogalapja az érintett hozzájárulása.

203. A felhasználó informatikai eszközén csak a felhasználó világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni (2003. évi C. törvény 155. § (4)

bekezdés alapján). A cookie adatok lejáratáról és harmadik személyek általi hozzáférésről is tájékoztatást kell adni.

204. A társaság honlapjának látogatásakor egy rövid összefoglalót kell adni a cookie-k alkalmazásáról, és egy linken keresztül elérhetővé kell tenni a tájékoztató teljes szövegét a **12. számú melléklet** szerint. A tájékoztatóval a társaság biztosítja, hogy a látogató a honlap szolgáltatásainak igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy a társaság mely adatkezelési célokból, mely adatfajtákat kezel, ideértve az igénybe vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.

205. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalmi szolgáltatások egyes kérdéseiről szóló 2001. CVIII. törvény (e-kertv) 13/A. § (3) bekezdése szerint a szolgáltató a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak az egyéb feltételek azonossága esetén úgy kell megválasztania és oly módon kell üzemeltetnie az alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez – a szükséges mértékben és ideig – indokolt.

27. Rendezvényeken készült képfelvételekkel kapcsolatos adatkezelés

206. Szakmai, kulturális, sport rendezvény szervezése esetén a társaság részéről a rendezvényen kép-, vagy kép- és hangfelvétel készülhet. Az adatkezelés jogalapja: az érintett hozzájárulása.

207. A kép- vagy kép- és hangfelvételeken történő részvétel kapcsán a képmásnak, mint személyes adatnak kezelésére – törvényi felhatalmazás hiányában – kizárólag az érintett előzetes hozzájárulásával kerülhet sor. Az érintettek hozzájárulását a **4. sz. melléklet** szerinti nyilatkozat kitöltésével kell megszerezni, kivéve, ha a felvétel:

a) nyilvános közéleti szereplés során készült felvételnek minősül,
b) tömegfelvételnek minősül, vagy
c) ha a felvétel a munkavállalóról technikai ellenőrzés keretében, a térfigyelő kamerákra vonatkozó rendelkezés szerint készül.

208. A hozzájáruló nyilatkozat aláírása önkéntes. Akik nem kívánnak a felvételeken szerepelni, e joguk érvényesítése érdekében – nevet, munkakört megjelölve – nyilvántartásba kell venni.

209. A hozzájáruló nyilatkozatokat a rendezvény szervezésre kijelölt személy összegyűjti, a nyilvántartást elkészíti és elzárva tárolja. A nyilvántartott neveket kizárólag a felvételekkel kapcsolatos adatkezelést végző személyek, valamint az adatvédelmi tisztviselő ismerheti meg.

210. A rendezvényen történő kép- és hangfelvétel készítése esetén a rendezvényért felelős feladata a rendezvény megkezdése előtt felhívni az érintettek figyelmét arra, hogy

amennyiben a képfelvétel készítéséhez – ide nem értve a tömegfelvételt és a nyilvános közéleti szereplést – nem járulnak hozzá, úgy azt jelezzék a jelenlévő fotós részére.

211. A jelenléti vagy regisztrációs ív alkalmazásával járó események esetén az adatkezelési tájékoztatót jól látható helyen elérhetővé kell tenni, és a jelenléti íven vagy regisztrációs adatlapon az adatkezelési hozzájárulásnak külön rubrikát kell kialakítani.

212. A személyes adatok kezelésének célja a társasági kohézió növelése, megfelelő munkahelyi légkör kialakítása.

213. Nincs szükség az érintett hozzájárulására a tömegfelvétel (ábrázolás módja nem egyéni, a felvétel összhatásában örökít meg a nyilvánosság előtt lezajlott eseményeket), illetve a közérdeklődésre számot tartó tudósítás, a jelenkor eseményeiről való szabad tájékoztatás esetén.

214. A személyes adatok a hozzájárulás visszavonásáig tárolhatók, más jogalap hiányában.

VII. RÉSZ

SZERZŐDÉS, MINT AZ ADATKEZELÉS JOGALAPJA

A szerződő felek adatainak kezelése

215. A társaság szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése, szerződési kedvezmény nyújtása céljából kezeli a vele vevőként, szállítóként szerződött természetes személy nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát, egyéni vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely, telephely címét, telefonszámát, e-mail címét, honlap-címét, bankszámlaszámát, vevőszámát (ügyfélszámát, rendelésszámát), online azonosítóját (vevők, szállítók listája, törzsvásárlási listák), Ezen adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződéskötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

216. A társaság szerződéses kapcsolatot jellemzően reklámtevékenység, reklámfelület értékesítés körében létesít, a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény 6. §, valamint az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) 162. § (2) bekezdése, a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről 1995. évi CXIX. törvény 3. §-a figyelembe vételével.

217. A személyes adatokat, a társaság kereskedelemmel, ügyfélszolgálattal kapcsolatos feladatokat ellátó munkavállalói, könyvelési, adózási feladatokat ellátó munkavállalói, és adatfeldolgozói kezelhetik.

218. A személyes adatok kezelésének időtartama: a szerződés megszűnését követő 8 év a számviteli iratok megőrzése céljából.

219. Az érintett természetes személlyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződésen alapul, amely tájékoztatás történhet a szerződésben is. Az érintettet személyes adatai adatfeldolgozó részére átadható, amelyről a szerződésben tájékoztatni kell. A természetes személlyel kötött szerződéshez kapcsolódó adatkezelési tájékoztató szövegét a **11. számú melléklet** tartalmazza.

28. A jogi személy partnerek kapcsolattartóinak elérhetőségi adatai

220. A társaság, az érintett természetes személy nevét, címét, telefonszámát, e-mail címét, online azonosítóját kezeli, jogalapja, a szerződés teljesítése, illetve az ehhez kapcsolódó munkáltatói érdek érvényesítése.

221. Az adatkezelők a szerződésben **11. számú mellékletben** nyilatkoznak arról, hogy olyan személyt jelölnek meg kapcsolattartónak, akinek ez munkaköri feladatainak ellátásához tartozik, és akit tájékoztattak arról, hogy az adatkezelő tevékenységével kapcsolatban más adatkezelők a munkáltató által biztosított eszközön, munkaidőben megkereshetik.

222. A személyes adatok kezelésének célja, a társaság jogi személy partnerével kötött szerződés teljesítése, üzleti kapcsolattartás.

223. A személyes adatok címzettjei, a társaság kereskedelemmel, ügyfélszolgálattal kapcsolatos feladatokat ellátó munkavállalói.

224. A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 5 évig.

VIII. RÉSZ

JOGI KÖTELEZETTSÉG TELJESÍTÉSÉN ALAPULÓ ADATKEZELÉSEK

29. Adó-, járulék- és számviteli kötelezettségek teljesítése céljából

225. A társaság jogi kötelezettség teljesítése alapján, törvényben előírt adó-, járulék és számviteli kötelezettségek teljesítése (könyvelés, adózás) céljából kezeli a vevőként,

szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait.

226. A kezelt adatok az általános forgalmi adóról szóló 2017. évi CXXVII. tv. 169. §, és 202. §-a alapján különösen: adószám, név, cím, adózási státusz, a számvitelről szóló 2000. évi C. törvény 167. §-a alapján: név, cím, a gazdasági műveletet elrendelő személy vagy szervezet megjelölése, az utalványozó és a rendelkezés végrehajtását igazoló személy, valamint a szervezettől függően az ellenőr aláírása; a készletmozgások bizonylatain és a pénzkezelési bizonylatokon az átvevő, az ellennyugtákon a befizető aláírása, a személyi jövedelemadóról szóló 1995. évi CXVII. törvény (továbbiakban: Szjatv.) alapján: vállalkozói igazolvány száma, őstermelői igazolvány száma, adóazonosító jel.

227. A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év.

228. Az alkalmazotti adatkezelésekre vonatkozóan a társaság külön tájékoztatót alkalmaz a **7. sz. melléklet** szerint.

229. A jelen címhez kapcsolódó személyes adatokat a társaság adózási, könyvviteli, bérszámfejtési, társadalombiztosítási feladatait ellátó munkavállalói és adatfeldolgozói kezelhetik.

30. Munkajogviszonyra vonatkozó adatkezelések

230. A társaság jogi kötelezettség teljesítése alapján, törvényben előírt munkajogviszony szabályszerű teljesítése céljából kezeli a munkavállalók törvényben meghatározott adatait.

231. Az alkalmazotti adatkezelésekre vonatkozóan a társaság külön tájékoztatót alkalmaz a **7. sz. melléklet** szerint.

232. A jelen címhez kapcsolódó személyes adatokat a társaság személyzeti feladatait ellátó munkavállalói, adatfeldolgozói, illetve közös adatkezelők kezelhetik.

31. Kifizetői adatkezelés

233. A társaság a törvényben előírt adó- és járulékkötelezettségek teljesítése (adó-, adóelőleg, járulékok megállapítása, bérszámfejtés, társadalombiztosítási, nyugdíj ügyintézés) céljából kezeli azon érintettek – munkavállalók, családtagjaik, foglalkoztatottak, egyéb juttatásban részesülők – adótörvényekben előírt személyes adatait, akikkel kifizetői (az adózás rendjéről szóló 2017. évi CL. törvény (Art.) 7. § 31. pontja) kapcsolatban áll. A kezelt adatok körét az Art. 50. §-a határozza meg, kiemelve ebből: a természetes személy természetes személyazonosító adatait (ideértve az előző nevet és a titulust is), nemét, állampolgárságát, a természetes személy adóazonosító jelét, társadalombiztosítási azonosító jelét (TAJ szám). Amennyiben az adótörvények ehhez jogkövetkezményt fűznek, a Társaság kezelheti a munkavállalók egészségügyi

(Szjatv. 40. §) és szakszervezeti (Szjatv. 47. § (2) bekezdés b) pontja) tagságra vonatkozó adatokat adó és járulékkötelezettségek teljesítés (bérszámfejtés, társadalombiztosítási ügyintézés) céljából.

234. Az alkalmazotti adatkezelésekre vonatkozóan a társaság külön tájékoztatót alkalmaz a **7. sz. melléklet** szerint.

235. A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év, nyugellátást érintő adatok esetén az öregségi nyugdíjkorhatárt követő 5 évig.

236. A személyes adatokat a társaság adózási, bérszámfejtési, társadalombiztosítási (kifizetői) feladatait ellátó munkavállalói és adatfeldolgozói kezelhetik.

32. A maradandó értékű iratokra vonatkozó adatkezelés

237. A társaság kezeli a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény szerint maradandó értékűnek minősülő iratait abból a célból, hogy irattári anyagának maradandó értékű része épségben és használható állapotban a jövő nemzedékei számára is fennmaradjon. Az adattárolás ideje: a közlevéltár részére történő átadásig.

238. A személyes adatokat a társaság vezetője, iratkezelést, irattározást végző munkavállalója, a közlevéltár munkatársa kezelheti.

33. A pénzmosás / terrorizmus finanszírozása elleni kötelezettségekhez, és korlátozó intézkedésekhez kapcsolódó adatkezelés

239. A társaság, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényben (Pmt.) meghatározott célból kezeli ügyfelei, ezek képviselői, és a tényleges tulajdonosok meghatározott adatait (családi utónevét, születési családi és utónevét, állampolgárságát, születési helyét, idejét, anyja születési nevét, lakcímét, ennek hiányában tartózkodási helyét, azonosító okmányának típusát és számát; lakcímet igazoló hatósági igazolványa számát). Az adatkezelés ideje a Pmt. 56. § (2) bekezdése alapján 8 év.

240. A társaság az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló 2017. évi LII. törvényben (Kit) meghatározott célból kezeli a törvényben meghatározott adatokat (családi utónevét, születési családi és utónevét, állampolgárságát, születési helyét, idejét, anyja születési nevét, lakcímét, ennek hiányában tartózkodási helyét, azonosító okmányának típusát és számát). Az adatkezelési idő a Kit. 16. § (5) bekezdése alapján 10 év.

241. A személyes adatokat a társaság vezetője, ügyfélkiszolgálással kapcsolatos feladatokat ellátó munkavállalói, a társaság által kijelölt személye jogosult.

34. Az adatfeldolgozás általános szerződési feltételei

242. A társaság az adatfeldolgozási tevékenységre írásbeli szerződést köt.

243. A társaság adatfeldolgozási tevékenységének általános szerződési feltételeit a **16. sz. melléklet** tartalmazza.

244. Az általános szerződési feltétel tartalmát a másik féllel a szerződéskötést megelőzően meg kell ismertetni, és azt a másik félnek el kell fogadnia.

IX. RÉSZ

JOGOS ÉRDEKEN ALAPULÓ ADATKEZELÉSEK

35. Közszolgálati médiaszolgáltatás

245. A társaság tevékenységéből adódóan médiaszolgáltatónak és sajtótermék kiadónak minősül, személyes adatokat kezel, amelyre Magyarország Alaptörvényében meghatározott a „Szabadság és felelősség" rész IX. cikke alapján és a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény alapján jogosult.

246. A közszolgálati médiaszolgáltatás érdekében folytatott adatkezelés kapcsán a társaság minden esetben mérlegeli a közvélemény megfelelő tájékoztatásához való jogot és az érintett személyhez fűződő jogát, és ennek megfelelően dönt az adatkezelésről. A társaság a jogszabályokban és etikai normákban foglaltaknak megfelelően folytatja tömegtájékoztatási tevékenységét. A társaság, így a GDPR 6. cikk (1) bekezdés f) pontja alapján kezeli az adatokat, illetve a GDPR 6. cikk (1) bekezdés c) pontja alapján jogi kötelezettség teljesítése érdekében megőrzi, nyilvántartja azokat a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény 83. § (3) bekezdés alapján.

X. RÉSZ

ADATVÉDELMI INCIDENSEK KEZELÉSE

36. Az adatvédelmi incidens fogalma

247. 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.

37. Adatvédelmi incidensek kezelés, orvoslása

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

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

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

251. A társaság munkavállalói kötelesek írásban jelezni a vezetőnek, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek.

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

253. Adatvédelmi incidens bejelentése esetén a társaság vezetője – az informatikai, pénzügyi és működési vezető bevonásával – haladéktalanul megvizsgálja a bejelentést.

254. Az előzetes vizsgálat során el kell dönteni, hogy valódi incidensről, vagy téves jelzésről van szó. Az előzetes vizsgálatba a vezető bevonja a rendszergazdát, szükség esetén az adatvédelmi tisztviselőt, illetve az adatfeldolgozót, valamint a személyes adat kezelésének ellenőrzésével megbízott személyt.

255. A kivizsgálás eredményéről a társság vezetője részére összefoglaló és döntési javaslat készül, valamint a feltárt hibák, hiányosságok orvoslására haladéktalanul intézkedni kell.

256. Meg kell vizsgálni és meg kell állapítani:
a) az incidens fajtáját
b) a bekövetkezésének időpontját és helyét,
c) az incidens körülményeit, hatásait,
d) az incidens során kompromittálódott adatok körét, számosságát,
e) a kompromittálódott adatokkal érintett személyek körét,
f) az incidens elhárítása érdekében tett intézkedések leírását,
g) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

257. Amennyiben az adatvédelmi incidenst be kell jelenteni a felügyeleti hatóság részére (NAIH), úgy erről a társaság vezetője dönt, és felkéri az adatvédelmi tisztviselőt az online rendszerben való rögzítésre.

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

259. Amennyiben az adatvédelmi incidens kapcsán bűncselekmény gyanúja merül fel, úgy a társaság büntetőfeljelentést tesz.

260. Az adatvédelmi incidensek megfelelő kezelését erre irányuló vezetői döntés esetén évente gyakorolni indokolt.

38. Adatvédelmi incidensek nyilvántartása

261. Az adatvédelmi incidensekről a **2. sz. melléklet** szerinti nyilvántartást kell vezetni, amely tartalmazza:

a) az incidens jellegét,
b) az érintett személyes adatok kategóriáit, számát,
c) az adatvédelmi incidenssel érintettek körét és számát,
d) az adatvédelmi incidensről történt tudomásszerzés időpontját, körülményeit,
e) az adatvédelmi incidens körülményeit, hatásait,
f) az adatvédelmi incidens orvoslására megtett intézkedéseket,
g) a bejelentés időpontját,
h) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

262. A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

39. Adatvédelmi incidens bejelentése a NAIH részére, illetve az érintettek tájékoztatása

263. Az adatvédelmi incidenseket nyilván kell tartani és amennyiben kockázatot jelentenek az érintettekre vonatkozóan, úgy a NAIH részére is be kell jelenteni. A társaság a NAIH honlapján elérhető online incindensbejelentő felületen regisztrál.

264. Az adatszolgáltatásnak tartalmaznia kell:

a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit, hatásait,
c) az incidens során kompromittálódott adatok körét, számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedések leírását,
f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

265. A Társaság indokolatlan késedelem nélkül tájékoztatja az érintetteket valamennyi olyan adatvédelmi incidensről, ami olyan személyes adatokat érint, amely tekintetében a Társaság Adatkezelőként jár el, és amely valószínűsíthetően magas kockázattal jár a

természetes személye jogaira és szabadságaira nézve. A Társaság az adatvédelmi incidensre vonatkozó tájékoztatásban világosan és közérthetően nyújt tájékoztatást az alábbiakról:

a) az adatvédelmi incidens jellege;
b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
c) az adatvédelmi incidensből eredő, valószínűsíthető következmények;
d) az általa az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

266. Nem kell azonban az érintetteket tájékoztatni, ha

a) a Társaság megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták;
b) a Társaság az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg; vagy
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé (ez esetben nyilvánosan közzétett információk útján tájékoztat)

40. Nem belső adatvédelmi incidens

267. 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.

XI. RÉSZ

ADATVÉDELMI HATÁSVIZSGÁLAT

41. Adatvédelmi hatásvizsgálat és előzetes konzultáció

268. Ha az adatkezelés a NAIH honlapján közzétett hatásvizsgálati jegyzékben szerepel, illetve 29. cikk szerinti munkacsoport WP 248. számú állásfoglalása alapján hatásvizsgálat köteles, mivel – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, 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 értékelhetőek.

269. 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.

270. Az adatvédelmi hatásvizsgálat szükségességének megállapításához az érintett szakterület megválaszolja az 1. függelékben foglalt kérdéseket.

271. 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 érintett szakterület írásban rögzíti.

272. Amennyiben az érintett szakterület 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 adatkezelő szerv vezetőjénél.

273. Az adatkezelő szerv vezetője 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.

274. 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.

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

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

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

278. 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.

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

XIV. RÉSZ

AZ ADATTOVÁBBÍTÁS SZABÁLYAI

42. Adatkezeléssel, adattovábbítással megbízott dolgozók

280. 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.

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

282. A betegek adatait felvehetik, nyilvántarthatják, továbbíthatják:
- ügyvezető
- megbízott munkatárs

283. A társaság által kezelt adatok szabályszerű megkeresés esetén továbbíthatók az adatok kezelésére jogosult hatóságok, bíróságok részére.

43. Hatósági megkeresések

284. 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 hivatali 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.

285. 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).

286. 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.

287. 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 a 284. pontban foglalt egyéb feltételek megléte.

288. 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)

44. Külföldi adattovábbítás

289. 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).

290. 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).[1]

291. 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.

292. 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.

293. 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:

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

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.

294. 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

45. Tájékoztatás az érintett jogairól

295. A társaság honlapján az érintettek jogairól tájékoztatót kell elhelyezni és azt folyamatosan karbantartani, amely tájékoztató jelen szabályzat **3. számú melléklet**e.

296. Az adatkezeléshez kapcsolódó igényeket a társaság vezetője részére be kell mutatni, aki gondoskodik arról, hogy határidőn belüli megválaszolásáról.

297. 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.

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

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

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

301. 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;

46. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának támogatása

302. 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 érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

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

304. 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.

305. 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.

306. 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.

47. Előzetes tájékozódáshoz való jog, ha a személyes adatokat az érintettől gyűjtik

307. Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelést megelőzően tájékoztatást kapjon az alábbiakról:

a) az adatkezelő és képviselője kilétéről és elérhetőségeiről,
b) az adatvédelmi tisztviselő elérhetőségeiről (ha van ilyen),
c) a személyes adatok tervezett kezelésének céljáról, az adatkezelés jogalapjáról,
d) jogos érdek érvényesítésén alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekeiről,
e) a személyes adatok címzettjeiről – akikkel a személyes adatot közlik - illetve a címzettek kategóriáiról, ha van ilyen;
e) annak tényéről, ha az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

308. A tisztességes és átlátható adatkezelés biztosítsa érdekében az adatkezelőnek az érintettet a következő kiegészítő információkról kell tájékoztatnia:
a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
b) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
c) az érintett hozzájárulásán alapuló adatkezelés esetén, a hozzájárulás visszavonásához való jogról, amely nem érinti a visszavonás előtt végrehajtott adatkezelés jogszerűségét;
d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
f) az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról, és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

309. Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet az eltérő célról és az előző pontban írt minden releváns kiegészítő információról.

48. Az érintett rendelkezésére bocsátandó információk, ha a személyes adatokat nem tőle szerezték meg

310. Ha az adatkezelő a személyes adatokat nem az érintettől szerezte meg, az érintettet az adatkezelőnek a személyes adatok megszerzésétől számított legkésőbb egy hónapon belül; ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor tájékoztatnia kell a megelőző cím első két pontjában írt tényekről és információkról, továbbá az érintett személyes adatok kategóriáiról, valamint a személyes adatok forrásáról és adott esetben arról, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

311. A további szabályokra a megelőző cím első két pontjában írtak irányadók.

49. Az érintett hozzáférési joga

312. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy a személyes adatokhoz és az Előzetes tájékoztatáshoz való jog kezdetű című 1. pontjában írt kapcsolódó információkhoz hozzáférést kapjon.

313. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére továbbítják, az érintett jogosult tájékoztatást kapni a GDPR 46. cikk szerinti továbbításra vonatkozó garanciákról.

314. Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel.

50. A helyesbítéshez való jog

315. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

316. Az adatkezelés céljára figyelemmel, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

317. A helyesbítés, kiegészítés gyakorlása esetén a megváltozott, illetve új adatok igazolását (bemutatását) kell kérni az érintettől.

51. A törléshez való jog („az elfeledtetéshez való jog")

318. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha

a) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelésre vonatkozó hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére közvetlenül gyermeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

319. A törléshez való jog nem gyakorolható, ha az adatkezelés szükséges

a) a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b) az adatkezelőre alkalmazandó jogi kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

c) a népegészségügy területét érintő közérdek alapján;

d) a közérdekű archiválási-, tudományos és történelmi kutatási-, vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

e) jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

52. Az adatkezelés korlátozásához való jog

320. Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha:

a) az érintett vitatja a személyes adatok pontosságát, ebben az esetben a korlátozás arra az időtartamra vonatkozik, amely alatt az adatkezelő ellenőrizheti a személyes adatok pontosságát;

b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és helyette kéri azok felhasználásának korlátozását;

c) az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d) az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

321. Az adatkezelés korlátozása esetén a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy személyek jogainak védelme érdekében, vagy fontos közérdekből lehet kezelni.

322. Az adatkezelés korlátozásának idejére intézkedni kell az adatokhoz való felhasználói hozzáférés megszüntetéséről, az érintett adat honlapról való eltávolításáról, illetve a papír alapú, illetve elektronikus tárolás megváltoztatásáról.

323. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

53. A helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

324. Az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről.

54. Az adathordozhatósághoz való jog

325. A társaság automatizált döntésen alapuló adatkezelést nem végez, ezért az adathordozhatósághoz való jog nem gyakorolható.

326. Az adathordozhatósághoz való jog az adatkezelő által feldolgozás eredményeként létrejövő adatok estén nem gyakorolható.

55. A tiltakozáshoz való jog

327. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak jogos érdeken alapuló kezelése ellen, ideértve a profilalkotást is. Ebben az esetben az adatkezelő az érdekmérlegelési tesztet ismét lefolytatja és a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

328. A személyes adatok közvetlen üzletszerzés érdekében történő kezelése esetén, az érintett jogosult arra, hogy tiltakozzon a rá vonatkozó személyes adatok kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

329. Az előző két pontban rögzített jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

330. Az információs társadalommal összefüggő szolgáltatásokhoz kapcsolódóan az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja, amelyre legkésőbb az első kapcsolatfelvétel során fel kell hívni az érintett figyelmét.

331. Ha a személyes adatok kezelésére tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

56. Automatizált döntéshozatal, profilalkotás

332. A társaság automatizált adatkezelést nem alkalmaz.

57. Korlátozások

333. Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel a GDPR 23. cikkben meghatározott esetekben korlátozhatja jogok és kötelezettségek (Rendelet 12-22. cikk, 34. cikk, 5. cikk) terjedelmét, hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

58. Tájékoztatás az adatvédelmi incidensről

334. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

335. Az adatvédelmi incidensről szóló tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

336. Az érintettet nem kell az tájékoztatni, ha:
a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

59. A felügyeleti hatóságnál (NAIH) történő panasztétel joga

337. Az érintett jogosult panaszt tenni a felügyeleti hatóságnál (Nemzeti Adatvédelmi és Információszabadság Hatóság), ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t. Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az ügyfél jogosult bírósági jogorvoslattal élni.

60. A felügyeleti hatósággal szembeni bírói jogorvoslat joga

338. Az egyéb jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

339. Az érintett jogosult a bírósági jogorvoslatra, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

340. A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

341. Ha a felügyeleti hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében az Európai Adatvédelmi Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.

61. Az adatkezelővel vagy az adatfeldolgozóval szembeni bírósági jogorvoslat joga

342. A rendelkezésre álló nem bírósági útra tartozó jogorvoslatok – köztük a felügyeleti hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak a GDPR-nak nem megfelelő kezelése következtében megsértették a jogait.

343. Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

XIII. RÉSZ

ZÁRÓ RENDELKEZÉSEK

62. A Szabályzat megállapítása, módosítása és beépítése

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

345. 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.

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

347. 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.

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

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

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

351. 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 jelen szabályzat **17. számú melléklete** tartalmazza.

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

353. A munkaszerződés módosításban a szabályzatban foglaltak be nem tartása esetére egy havi alapbéréig terjedő szankció állapítható meg, amennyiben a munkavállaló által okozott adatvédelmi incidenst legalább az adatvédelmi felügyeleti hatóság (NAIH) részére be kell jelenteni.

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

355. 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 három munkanapon belül adatvédelmi oktatásban részesíteni és részére a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani, majd az oktatást követő egy héten belül vizsgáztatásukat elvégezni.

356. A társaság személyes adatok kezelő állománya évente adatvédelmi oktatáson vesz részt, amelyet adatvédelmi tisztviselő tart. Az éves oktatás során incidenskezelési gyakorlat megtartására is sor kerülhet (nem valós adatokkal).

357. 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.

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

359. Jelen szabályzat és annak mellékletei dr. Kozma Gergely e.v. szellemi terméke, aki fenntart minden jogot ide értve 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 elő-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 hatóköréhez 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.