A Büll & Strunz Kft.

adatkezelési és adatbiztonsági szabályzata

I. A szabályzat hatálya

1. Jelen szabályzat hatálya kiterjed a Büll & Strunz Kft. vállalkozás teljes egészére, valamennyi szervezeti egységére és az összes foglalkoztatottjára (a továbbiakban: vállalkozás).

II. A szabályzat célja

2. A Szabályzat célja, hogy biztosítsa a személyes adatok „*Az Európai Unió Általános Adatvédelmi Rendelet*” (679/2016 sz. rendelet, a továbbiakban: GDPR) szerinti védelmének érvényesülését, az információs önrendelkezés megvalósulását, továbbá, hogy a vállalkozás által kezelt személyes adatok tekintetében meghatározza az adatkezelés során irányadó adatvédelmi és adatbiztonsági szabályokat.

III. Irányadó jogszabályok

3. A vállalkozásnak az adatkezelése során az alábbi jogszabályokban foglalt előírásoknak megfelelően kell eljárnia, a jelen belső szabályzatban foglaltak szerint:

- Az Európai Parlament és a Tanács (Eu) 2016/679 Rendelete (2016. április 27.)

a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: GDPR)

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)
- a polgári törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.)
- a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.)

IV. Az adatkezelés alapelvei

4. A vállalkozás az adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi (jogszerűség, tisztességes eljárás és átláthatóság).

5. A vállalkozás a személyes adatok gyűjtését csak meghatározott, egyértelmű és jogszerű célból végzi, és azokat nem kezeli ezekkel a célokkal össze nem egyeztethető módon (célhoz kötöttség).

6. A vállalkozás az adatkezelést annak célja(i) szempontjából megfelelően és relevánsan, és a szükségesre korlátozva végzi (adattakarékosság). Ennek megfelelően a vállalkozás nem gyűjt, és nem tárol több adatot, mint amennyi az adatkezelés céljának a megvalósulásához feltétlenül szükséges.

7. A vállalkozás adatkezelése pontos és naprakész. A vállalkozás minden észszerű intézkedést megtesz annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul törlésre vagy helyesbítésre kerüljenek (pontosság).

8. A vállalkozás a személyes adatokat olyan formában tárolja, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, figyelemmel a vonatkozó jogszabályokban meghatározott tárolási kötelezettségre (korlátozott tárolhatóság).

9. A vállalkozás megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítja a személyes adatok megfelelő biztonságát, ideértve a személyes adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet (integritás és bizalmas jelleg).

10. A vállalkozás felelős a fentiekben részletezett alapelveknek való megfelelésért, továbbá a vállalkozás igazolja ezen megfelelést (elszámoltathatóság). Ennek értelmében a vállalkozás gondoskodik a jelen belső szabályzatban foglaltak folyamatos érvényesüléséről, az adatkezelésének folyamatos felülvizsgálatáról és szükség esetén az

adatkezelési eljárások módosításáról, kiegészítéséről. A vállalkozás a jogszabályi kötelezettségeknek való megfelelés igazolására dokumentációt készít.

V. Adatkezelési jogalapok

11. A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább a 12-17. pontokban meghatározott jogalapok egyike teljesül:

12. Az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez (a továbbiakban: hozzájáruláson alapuló adatkezelés).

13. Az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (a továbbiakban: szerződésen alapuló adatkezelés).

14. Az adatkezelés a vállalkozásra vonatkozó jogi kötelezettség teljesítéséhez szükséges (a továbbiakban: jogi kötelezettségen alapuló adatkezelés).

15. Az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (a továbbiakban: létfontosságú érdeken alapuló adatkezelés).

16. Az adatkezelés a vállalkozás vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek (a továbbiakban: jogos érdeken alapuló adatkezelés).

17. A vállalkozás egy adott személyes adatkör kezelése vonatkozásában mindig csak egy jogalap alapján végzi az adatkezelést. Az adatkezelés jogalapja az adatkezelés során változhat.

VI. Az adatvagyon leltár

18. A vállalkozás a tevékenysége körében végzett adatkezelésre vonatkozó, a GDPR és a jogszabályok által előírt kötelezettségeknek megfelelő technikai és szervezési intézkedések megalkotása céljából adatvagyon leltárt készít. Az adatvagyon leltár tartalmazza a vállalkozás által kezelt összes adatkört.

19. A vállalkozás adatkezelési tevékenységével összefüggésben az adatvagyon leltárban meghatározásra kerülnek az alábbiak:

a) az adattípus *[például név, lakcím, telefonszám, e-mail cím, munkabér]*

b) az adatkezelés megnevezése és célja *[például jogszabályi kötelezettség teljesítése, szerződés teljesítése, munkahelyi adatkezelés]*

c) az adatkezelés jogalapja *[például szerződés, jogszabály, jogos érdek]*

d) az adat forrása *[kitől származik az adat]*

e) hol tárolják az adatot *[például számítógépes program adatbázisa, számítógép, papír alapon adminisztrációt végző munkatárs]*

f) ki, kik számára kerülhet az adat továbbításra *[például hatóság].*

20. A vállalkozás adatfeldolgozási tevékenységével összefüggésben meghatározásra kerülnek az alábbiak:

a) mely tevékenységéhez kötötten minősül a vállalkozás adatfeldolgozónak;

b) ki az adatkezelő, akinek a nevében az adatfeldolgozási tevékenységet végzi;

c) milyen személyes adatokhoz fér hozzá;

d) mennyi ideig tárolhatja a személyes adatokat.

VII. Az érintett jogai és azok érvényesítése

21. A vállalkozás a GDPR rendelkezéseivel összhangban az alábbiakat biztosítja az érintettek számára.

Tájékoztatáshoz való jog

22. A tájékoztatáshoz való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

23. A vállalkozás tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújt tájékoztatást az érintettek számára.

24. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni.

Tájékoztatás az érintett kérésére

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

26. A vállalkozás indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 30 napon belül tájékoztatja az érintettet az egyéb érintetti jogokra vonatkozó érintetti kérelem nyomán hozott intézkedésekről.

27. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, a 30 napos határidő további 60 nappal meghosszabbítható. A határidő meghosszabbításáról a vállalkozás a késedelem okainak megjelölésével a kérelem kézhezvételétől számított 30 napon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a

kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

28. A tájékoztatást és intézkedést díjmentesen kell biztosítani.

29. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, úgy a vállalkozás, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

a) észszerű összegű díjat számíthat fel, vagy

b) megtagadhatja a kérelem alapján történő intézkedést.

30. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a vállalkozást terheli.

Kötelező tájékoztatás

31. Amennyiben a vállalkozás az adatokat közvetlenül az érintettől szerezte meg (ide értve különösen az ügyfeleket), úgy a vállalkozás mindenképpen tájékoztatást nyújt az alábbiakról:

a) a vállalkozás képviselőjének a kiléte és elérhetőségei;

b) az adatvédelmi tisztviselő elérhetőségei, amennyiben ilyennel rendelkezik;

c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;

d) a jogos érdeken alapuló adatkezelés esetén, a vállalkozás vagy harmadik fél jogos érdekei;

e) adott esetben a személyes adatok címzettjei;

f) adott esetben annak ténye, hogy a vállalkozás harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

32. A személyes adatok első megszerzésének időpontjában a vállalkozás a fentieken túl az érintetteket tájékoztatja az alábbiakról is:

a) a személyes adatok tárolásának időtartamáról

b) az érintett azon jogáról, hogy kérelmezheti a vállalkozástól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, egyes jogalapokhoz tartozó adatkezelés esetében törlését vagy kezelésének korlátozását, és egyes jogalapokhoz tartozó adatkezelés esetében tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;

c) a hozzájáruláson alapuló adatkezelés bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

d) a felügyeleti hatósághoz (Nemzeti Adatvédelmi Hatóság, továbbiakban: Hatóság vagy NAIH) 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 következményekkel járhat az adatszolgáltatás elmaradása.

33. Ha a vállalkozás a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és a 32. pontban említett minden releváns kiegészítő információról.

34. A vállalkozás a kötelező tájékoztatásnak többféle módon tehet eleget.

a) A 32. pontban foglalt információkat a vállalkozás ("Adatkezelési tájékoztató" címen) közzéteszi a honlapján, olyan módon, hogy az könnyen megtalálható és könnyen elérhető legyen bárki számára.

b) A honlapon való közzététel mellett vagy helyett, a vállalkozás választhatja az "Adatkezelési tájékoztató" szerződés mellékleteként történő hozzáférhetővé tételét. Ebben az esetben elegendő az adott érintetti körre vonatkozó adatkezelési tájékoztatást az érintett rendelkezésére bocsátani. Általános Szerződési Feltétel (ÁSZF) részét nem képezheti az "Adatkezelési tájékoztató".

Hozzáférés joga

35. A hozzáférés joga minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

36. Az érintett jogosult arra, hogy a vállalkozástól visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek kategóriái, akikkel a személyes adatokat a vállalkozás közölte vagy közölni fogja

d) adott esetben a személyes adatok tárolásának tervezett időtartama

e) az érintett azon joga, hogy kérelmezheti a vállalkozástól a rá vonatkozó személyes adatok helyesbítését, egyes jogalapokhoz kötött adatkezelés esetén ezen adatok törlését vagy kezelésének korlátozását, és egyes jogalapokhoz kötött adatkezelés esetén tiltakozhat az ilyen személyes adatok kezelése ellen;

f) a felügyeleti hatósághoz címzett panasz benyújtásának joga;

g) ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;

h) az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

37. A vállalkozás az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja.

38. Az érintett által kért további másolatokért a vállalkozás az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, melynek mértékét a vállalkozás árszabási szabályzata, egyéb szabályzata, vagy egyéb dokumentum tartalmazza.

Helyesbítéshez való jog

39. A helyesbítéshez való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

40. A vállalkozás, az érintett erre irányuló kérelme esetén indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozóan pontatlanul kezelt személyes adatokat. Az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését.

Törléshez (elfeledtetéshez) való jog

41. A törléshez (elfeledtetéshez) való jog nem illeti meg az érintettet automatikusan, minden jogalaphoz kapcsolódó adatkezelés vonatkozásában.

42. A vállalkozás indokolatlan késedelem nélkül törli az érintettre vonatkozó személyes adatokat, ha az alábbi indokok valamelyike fennáll:

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

b) az érintett visszavonja az adatkezelés alapját képező hozzájárulását (hozzájáruláson alapuló adatkezelés esetén), és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre a 16. pont szerint alkalmazott adatkezelés jogalap esetében (jogos érdeken alapuló adatkezelés)

d) a személyes adatok jogellenesen kerültek kezelésre;

e) a személyes adatokat a vállalkozásra alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

43. Az érintett törlési kérelmének a vállalkozás nem tesz eleget, amennyiben az adatkezelés szükséges a személyes adatok kezelését előíró, a vállalkozásra alkalmazandó jogszabályi kötelezettség teljesítéséhez.

44. Amennyiben a vállalkozáshoz törlési kérelem érkezik, a vállalkozás első lépésként megvizsgálja, hogy a törlési kérelem valóban a jogosulttól származik-e. Ennek érdekében a vállalkozás elkérheti az érintett és a vállalkozás között fennálló szerződés azonosítására szolgáló adatokat (például szerződésszám, szerződés kelte), az érintett számára a vállalkozás által kiállított irat azonosítószámát, az érintettről nyilvántartott személyazonosító adatok megadását (a vállalkozás azonban nem kérhet azonosításként olyan plusz adatot, amelyet az érintettről nem tart nyilván).

45. Amennyiben a vállalkozásnak eleget kell tennie a törlési kérelemnek, úgy köteles mindent megtenni annak érdekében, hogy a személyes adat az összes adatbázisból törlésre kerüljön.

46. A vállalkozás a törlésről jegyzőkönyvet vesz fel annak érdekében, hogy a törlés megtörténtét igazolni tudja. A jegyzőkönyvet a vállalkozás képviselője vagy az a személy(ek) írja(ák) alá, aki(k)nek erre a munkaköri leírása nyomán jogosultsága van. A törlési jegyzőkönyv tartalmazza:

a) az érintett nevét

b) a törölt személyes adattípust

c) a törlés időpontját.

47. A vállalkozás tájékoztatja a törlési kötelezettségről mindazokat, akik számára a személyes adat továbbításra került.

Az adatkezelés korlátozáshoz való jog

48. A korlátozáshoz való jog minden adatkezelési jogalap vonatkozásában megilleti az érintettet.

49. A vállalkozás az érintett kérésére korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a) az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy a vállalkozás ellenőrizze a személyes adatok pontosságát;

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

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

f) az érintett a 16. pont szerint alkalmazott adatkezelés jogalap esetében (jogos érdeken alapuló adatkezelés) tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a vállalkozás jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

50. Ha az adatkezelés az előző pont alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

51. A vállalkozás tájékoztatja a kötelezettségről mindazokat, akik számára a személyes adat továbbításra került.

Tiltakozás

52. A tiltakozás joga az érintettet a jogos érdeken alapuló adatkezelési jogalap esetében illeti meg.

53. A vállalkozás az érintett tiltakozás iránti kérelme esetén a személyes adatokat nem kezelheti tovább, kivéve, ha 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.

54. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen.

55. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Adathordozhatósághoz való jog

56. Az adathordozhatósághoz való jog a hozzájáruláson vagy a szerződésen alapuló adatkezelés jogalap esetében illeti meg az érintettet, ha az adatkezelés automatizált módon történik.

57. A vállalkozás biztosítja, hogy érintett a rá vonatkozó, általa a vállalkozás számára rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá, hogy ezeket az adatokat az érintett egy másik adatkezelőnek továbbítsa.

VIII. Adatkezelési tevékenységek nyilvántartása

58. Az adatkezelési tevékenységek nyilvántartását a vállalkozás az elszámoltathatóság elvéből következően annak érdekében végzi, hogy az GDPR-nak való megfelelést nyomon tudja követni, és igazolni tudja.

59. A vállalkozás a felelősségébe tartozóan végzett adatkezelési tevékenységekről legalább az alábbi nyilvántartásokat vezeti:

a) adattovábbítás nyilvántartása

b) érintetti jogok érvényesítése iránti kérelmek és az arra a vállalkozás által adott válaszok nyilvántartása

c) hatósági megkeresések és az arra a vállalkozás által adott válaszok nyilvántartása

d) adatkezelés megszüntetése iránti kérelmek nyilvántartása

e) ügyfelek nyilvántartása

f) marketing célú megkeresések nyilvántartása

g) munkaviszonnyal összefüggő személyes adatok kezelésének nyilvántartása

h) munkaerő-felvétel nyilvántartása

i) adatvédelmi incidensek nyilvántartása.

60. Amennyiben a vállalkozás adatfeldolgozóként is végez tevékenységet, úgy a vállalkozás nyilvántartást vezet a vállalkozás nevében végzett adatfeldolgozói tevékenységek valamennyi kategóriájáról.

61. A nyilvántartásokat a vállalkozás írásban vezeti, papír alapon vagy elektronikus formátumban.

IX. Adatbiztonsági rendelkezések

62. A vállalkozás a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

63. Előzőek értelmében a vállalkozás köteles garantálni az általa kezelt adatok bizalmasságát, sérthetetlenségét és rendelkezésre állását.

64. A megfelelő szintű adatbiztonsági intézkedések meghatározása érdekében a vállalkozás a kezelésében lévő minden egyes adatállományt a védelmi igény szempontjából értékel, és biztonsági fokozatba sorol.

65. Az egyes adatkezelések biztonsági fokozatának megállapításához elemezni kell:

a) a kezelt személyes adatok jogosulatlan megismerésével, megváltoztatásával, törlésével, a hardver- és szoftvereszközök megrongálásával járó kockázatot és a várható kárt;

b) azt, hogy helyreállítható-e a sérült adatállomány, valamint az esetleges helyreállítás ráfordításait, a személyes adatok reprodukálásához szükséges adatforrások rendelkezésre állását, a manuális háttérnyilvántartásból az elveszített adatok pótlásának lehetőségét;

c) azt, hogy a kezelt személyes adatok jellegére tekintettel indokolt-e megkülönböztetett biztonsági előírásokat alkalmazni;

d) az adatbiztonságot veszélyeztető más kockázati elemeket;

66. Az adatkezelés biztonsága megvalósítása érdekében a vállalkozás fizikai, logikai és adminisztratív kontrollokat alkalmaz együttesen.

67. A vállalkozás legalább az alábbi fizikai kontrollokat alkalmazza:

a) a vállalkozás biztosítja, hogy épületébe/irodájába jogosulatlan személyek ne léphessenek be *[egyszerű kulcsos beléptetés, ahol a kulcs csak belépésre jogosultaknak áll rendelkezésre+ riasztó rendszer]*

b) a vállalkozás az általa mind elektronikusan, mind pedig papír alapon kezelt adatokhoz való jogosulatlan hozzáférés elkerülése érdekében biztosítja, hogy a kezelt adatokhoz fizikailag ne férhessen hozzá arra jogosulatlan személy *[irodák, szerver szobák zárása; monitor fóliák alkalmazása; monitorok olyan módon történő elhelyezése, hogy az azon szereplő adatokra kizárólag a jogosultak láthassanak rá; csak a vállalkozás által auditált adathordozót lehessen a számítógépekhez csatlakoztatni; vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja].*

68. A vállalkozás legalább az alábbi logikai kontrollokat alkalmazza:

a) a vállalkozás biztosítja, hogy az általa kezelt adatokhoz kizárólag az arra megfelelő jogosultsággal rendelkezők férjenek hozzá *[jogosultsági szintek meghatározása munkakörönként; számítógépes adatbázisokhoz való hozzáférés jogosultsági szinteknek megfelelő beállítása; a belső számítógépes hálózatba való belépés felhasználó névhez és jelszóhoz kötése; vagy bármi más, olyan módszer, amely a cél megvalósulását biztosítja]*

69. A vállalkozás legalább az alábbi adminisztratív kontrollokat alkalmazza:

a) a vállalkozás biztosítja, hogy a személyes adatokhoz való esetleges hozzáférés dokumentációkban nyomon követhető legyen *[tevékenység logolás]*

b) a vállalkozás biztosítja olyan iratkezelési eljárásrend kialakítását, hogy a hozzá tévesen beérkező személyes adatokat tartalmazó iratok a lehető leghamarabb kiszűrésre kerüljenek és azokat a lehető legszűkebb személyi kör ismerje meg. *[amennyiben a postabontó úgy*

ítéli meg, hogy ilyen adatot tartalmazó irat birtokába jutott, úgy azt további megismerés nélkül visszazárja, és egyeztetés végett felveszi a kapcsolatot a küldővel]

X. Adatvédelmi incidensek kezelése

70. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

71. Az adatvédelmi incidenst a vállalkozás indokolatlan késedelem nélkül, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott bejelenti a hatóságnak.

72. Az adatvédelmi incidenst nem kell a hatóságnak bejelenteni, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

73. Amennyiben a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

74. Amennyiben az adatvédelmi incidens hatóság számára történő bejelentése szükséges, úgy a bejelentésben:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát,

valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell a vállalkozás által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

76. A 75. pont szerinti tájékoztatásban az érintettel világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a 74. pont b)-d) alpontjaiban foglaltakat.

77. Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) a vállalkozás 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) a vállalkozás 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.

78. Amennyiben a vállalkozás adatfeldolgozási tevékenységet is végez, úgy a nála bekövetkezett adatvédelmi incidensről haladéktalanul tájékoztatja az adatkezelőt, akinek a számára az adatfeldolgozási tevékenységet végzi.

79. Amennyiben a vállalkozás adatfeldolgozót alkalmaz, úgy az adatfeldolgozó szerződésben ki kell kötni, hogy az adatfeldolgozó köteles a nála bekövetkezett adatvédelmi incidenst a hatósághoz történő bejelentéssel egyidejűleg - haladéktalanul bejelenteni a vállalkozásnak is.

XI. Ügyfél adatok kezelése

80. A vállalkozás tevékenységét írásbeli szerződés alapján végzi. Az adatok kezelésének jogalapja a szerződésen alapul, a szerződést aláíró félre vonatkozó személyes adatok vonatkozásában.

81. Az előző pont szerinti szerződés teljesítése keretében a vállalkozás számára hozzáférhetővé váló személyes adatok (így például a szerződésben szereplő kapcsolattartó adatai vagy a szerződés szerinti feladat ellátás során megismerni szükséges vagy szükségesnek ítélt személyes adatok) kezelésének jogalapja magán a szerződésen alapul. A GDPR rendelkezéseinek megfelelően ez esetben szükséges az alábbi érdekmérlegelési tesztet elvégezni:

a) adatkezelés tárgya

b) a jogos érdek jogalap megállapítása

c) a kezelendő személyes adatok

d) adatkezelés célja

e) a vállalkozás jogos érdekének megnevezése

f) az érintettek milyen jogai sérülhetnek

g) érdekmérlegelés

h) milyen intézkedéseket, garanciákat alkalmaz a vállalkozás az így gyűjtött személyes adatok megfelelő védelme érdekében.

82. Az adott személyes adat körének kezelésére vonatkozóan elvégzett érdekmérlegelési teszt(ek) jelen szabályzat mellékletét képezi(k).

XII. Munkaviszonnyal összefüggő adatkezelések

83. A vállalkozás a 34. pont szerinti "Adatkezelési tájékoztatója" vonatkozik az álláspályázatokra is. A vállalkozás az általa kiírt álláspályázatban az elérhetőség megjelölésével hivatkozik az "Adatkezelési tájékoztatóra".

84. Amennyiben a vállalkozás az állás betöltését követően is tárolni kívánja az állást el nem nyert álláspályázó által beadott iratokat, úgy ehhez az álláspályázó hozzájárulását kell kérni. A hozzájárulásnak önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Ennek érdekben a hozzájáruló nyilatkozatnak legalább az alábbiakat kell tartalmaznia:

a) a vállalkozás képviselőjének kiléte és elérhetőségei;

b) a személyes adatok tervezett kezelésének célja *[például későbbi megkeresés újonnan megnyílt pozíció betöltésére]*, valamint az adatkezelés jogalapja (hozzájáruláson alapuló);

c) a személyes adatok tárolásának időtartama;

d) az érintett azon joga, hogy kérelmezheti a vállalkozástól a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását;

e) az érintett azon joga, hogy bármely időpontban visszavonhatja a hozzájárulását, amely azonban nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

f) a hatósághoz címzett panasz benyújtásának jogáról.

85. A pályázat elbírálása után az eredménytelen pályázók személyes adatait tartalmazó adathordozókat a pályázónak – kérésére – 90 napon 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.

86. A vállalkozás a munkavállalók adatait a Mt. vonatkozó rendelkezései alapján kezeli és az Mt-ben meghatározott módon tájékoztatja, a GDPR-ban foglalt adatkezelési alapelvek betartása mellett.

87. A vállalkozás a munkavállalóknak tájékoztatást ad az általa igénybe vett adatfeldolgozókkal kapcsolatban azok kilétéről és a számukra továbbított adatok köréről.

88. A munkaviszonyban történő adatkezelés során jellemzően az alábbi jogalapok merülhetnek fel:

a) szerződésen alapuló *[a munkaszerződés]*

b) jogi kötelezettségen alapuló *[például adózás, tartásdíj levonás]*

c) jogos érdeken alapuló *[például munkahelyi ellenőrzéssel kapcsolatos adatok].*

89. Amennyiben a vállalkozás 88. c) pont alapján kezel adatot, úgy a GDPR rendelkezéseinek megfelelően ez esetben szükséges az alábbi érdekmérlegelési tesztet elvégezni:

i) a vállalkozás jogos érdekének megnevezése

j) kik az érintettek és milyen jogai sérülnek

k) érdekmérlegelés

l) milyen intézkedéseket, garanciákat alkalmaz a vállalkozás az így gyűjtött személyes adatok megfelelő védelme érdekében.

90. Az adott személyes adat körének kezelésére vonatkozóan elvégzett érdekmérlegelési teszt(ek)et a munkavállalók számára hozzáférhetővé kell tenni *[például belső hálózat útján, munkaszerződés mellékleteként].*

XIII. Az adatfeldolgozó igénybevételére vonatkozó rendelkezések

91. Ha az adatkezelést a vállalkozás nevében más végzi *[például bérszámfejtés, szerver szolgáltatás, honlap üzemeltetés]*, a vállalkozás kizárólag olyan adatfeldolgozókat vehet igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatfeldolgozás GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

92. Az adatfeldolgozó a vállalkozás előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.

93. Az adatfeldolgozó által végzett adatfeldolgozás vonatkozásában a vállalkozás és az adatfeldolgozó szerződést kötnek. Ezen szerződés az adatfeldolgozás tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint a vállalkozás kötelezettségeit és jogait határozza meg.

94. Az előző pont szerinti szerződés különösen előírja, hogy az adatfeldolgozó:

a) a személyes adatokat kizárólag a vállalkozás írásbeli utasításai alapján dolgozza fel,

b) biztosítja azt, hogy a személyes adatok feldolgozására feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) alkalmazza a legalább a vállalkozás által előírt szintű adatbiztonsági intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan fentebb említett feltételeket;

e) az adatfeldolgozás jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a vállalkozást abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti a vállalkozást az adatvédelmi incidens szerinti kötelezettségek teljesítésében, figyelembe véve az adatfeldolgozás jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) vállalja, hogy a nála bekövetkező adatvédelmi incidens esetén haladéktalanul tájékoztatja erről a vállalkozást;

h) az adatfeldolgozási szolgáltatás nyújtásának befejezését követően a vállalkozás döntése alapján minden személyes adatot töröl vagy visszajuttat a vállalkozásnak, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő.

95. Az adatfeldolgozó és a nála személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag a vállalkozás utasításának megfelelően kezelheti.

XIV. Hatályba léptető és záró rendelkezések

96. A jelen szabályzat 2018. május 28. napján lép hatályba.

Budapest, 2018. május hó 27. napja

Smoling László

ügyvezető