



**Békéscsabai
Szakképzési
Centrum**

OM azonosító: 203029

E/2020/000209

5600 Békéscsaba, Gyulai út 32/1.

Tel.: +36 66/441-314

Fax: +36 66/441-314

www.bszc.hu

E-mail: centrum@bszc.hu

NSRFH/602/0001862/2025

A Békéscsabai Szakképzési Centrum Adatvédelmi és Adatbiztonsági Szabályzata

Jóváhagyta:

.....
Uhljár Erik Róbert
kancellár



.....
Mucsi Balázs Sándor
főigazgató

Hatályos: 2025. szeptember 1-től
Érvényes: visszavonásig

1. A SZABÁLYZAT CÉLJA

1.1. Az adatvédelmi és adatbiztonsági szabályzat célja a Békéscsabai Szakképzési Centrum (a továbbiakban: Centrum) tevékenységével összefüggésben a személyes adatok védelméhez fűződő jog érvényesülésének biztosítása, a Centrum által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása, a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírások meghatározása.

1.2. A szabályozás az alábbi jogszabályokra, ajánlásokra és irányelvekre, belső szabályozásokra alapozva, azokkal teljes összhangban került kialakításra:

- 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)
- Magyarország Alaptörvényének VI. cikke,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény,
- a személy és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: vagyonvédelmi tv.),
- a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.),
- az elektronikus hírközlésről szóló 2003. évi C. törvény,
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény,
- a Nemzeti Adatvédelmi és Információszabadság Hatóság 2013. január 23-án kiadott ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről.

2. HATÁLY- ÉS FELELŐSSÉG MEGHATÁROZÁSA

2.1. Személyi hatály

A szabályzat személyi hatálya kiterjed a Centrum szervezeti egységeire, munkavállalóira, valamint a Centrumnál szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve titoktartási nyilatkozatokban rögzített mértékben.

2.2. Tárgyi hatály

Tárgyi hatálya kiterjed a Centrum szervezeti egységeinél folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás teljesen, vagy részben automatizált eszközzel, vagy manuális módon történik.

2.3. A szabályzat módosítása

A szabályzat elkészítése és szükség szerinti módosítása a Centrum belső adatvédelmi kapcsolattartójának (a továbbiakban: adatvédelmi kapcsolattartó) a feladata, szorosan együttműködve a Centrum külső adatvédelmi szakemberével.

3. FOGALOMMEGHATÁROZÁSOK

A szabályzat alkalmazása során – összhangban az Infotv., valamint az Mt. előírásaival – a következőkben meghatározott fogalmak irányadók:

- 3.1. **adat:** valamilyen jelrendszerben ábrázolt jelek, vagy elemi jelek sorozata, amelyeknek jelentésük, értelmük van, valamire vonatkoznak, valamit leírunk velük. Az adatok teljes információtartalmát adatkörnyezetük határozza meg, így az adat jelentésétől megfosztott információ.
- 3.2. **adatállomány:** az egy nyilvántartásban kezelt adatok összessége.
- 3.3. **adatbázis:** az adatok szervezett gyűjteménye, amelyet egy – az adatok tárolására, lekérdezésére és szerkesztésére alkalmas – szoftvereszköz kezel. Az adatbázis lényege, hogy az adatok mellett az adatok között lévő kapcsolatokat is tárolja. Az adatbázis fogalmát meg kell különböztetni az adatbázis-kezelőtől, amely az adatbázis működtetésére, rendszerszintű és felhasználói folyamatok szervezésére szolgáló szoftver eszköz (program).
- 3.4. **adatszoport:** Adatok, (azaz tények, koncepciók vagy utasítások formalizált megjelenítése, rögzített jelsorozat, beszéd vagy technikai eszközökkel történő közlés, értelmezés és feldolgozás számára. Jelen Szabályzatban írásban vagy elektronikus úton készített – bármilyen adathordozón tárolt – szöveg, számadatsor, tény, információ, vázlat, grafikon, kép és ábra) és adatkörök összefoglaló elnevezése, általában nyilvántartási funkció alapján.
- 3.5. **adatbiztonság:** az informatikai (adattároló és feldolgozó) rendszer azon állapota, amelyben az adatok elvesztésének illetve megsemmisülésének kockázata a megfelelő intézkedésekkel elviselhető mértékűre csökkenthető. Ez az állapot olyan nemzetközi szabványokon alapuló előírások és megelőző biztonsági intézkedések betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és megbízhatóságát érintik.
- 3.6. **adattfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a feladatot az adaton végzik;
- 3.7. **adattfeldolgozó:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.
- 3.8. **adathordozó:** Az adat fizikai megjelenési formája, tárolási helye, ide értve az iratokat is.
- 3.9. **adatkezelés:** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
- 3.10. **az adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- 3.11. **adatkezelő:** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adattfeldolgozóval végrehajtatja.
- 3.12. **adatkör:** az adatfajták nevesített felsorolása. A felhasználás szempontjából funkcionálisan összetartozó üzleti adatok, azaz olyan halmaz, amely logikai szinten egységesen kezelhető, illetve kezelendő és a halmaz elemeinek védelmi igénye közel egy szinten van. (Pl.: Kassza Rendszer adatok, készpénz átutalási adatok).
- 3.13. **adatmegsemmisítés:** Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.
- 3.14. **adattovábbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
- 3.15. **adattörlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- 3.16. **adatmegjelölés:** az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

3.17. **adattvédelem:** a személyes adat jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

3.18. **adattvédelmi incidens:** személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

3.19. **álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

3.20. **adattvédelmi kapcsolattartó:** az adatkezelő által megbízott, az adattvédelmi ismeretek terén kellő tájékozottsággal rendelkező munkavállaló, aki részt vesz az adatkezelést érintő feladatok végrehajtásában és kapcsolatot tart az adattvédelmi kapcsolattartóval;

3.21. **adattzárolás:** az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

3.22. **anonimizálás:** olyan technikai eljárás, amely biztosítja az érintett és az adat közötti kapcsolat helyreállítási lehetőségének végleges kizárását.

3.23. **bűnügyi személyes adat:** a büntetőeljárás során vagy azt megelőzően, a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

3.24. **cookie:** (süti): rövid adatfájl, melyek a meglátogatott honlap helyez el a felhasználó számítógépén, abból a célból, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolható. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl. egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Tekintve, hogy a cookie segítségével nyomon követhetők a felhasználó böngészési szokásai, ezért azt kizárólag a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni.

3.25. **direkt marketing (közvetlen üzletszerzési) tevékenység:** azoknak a közvetlen megkeresés módszerével végzett tájékoztató tevékenységeknek és kiegészítő szolgáltatásoknak az összessége, amelyeknek célja az érintett részére termékek vagy szolgáltatások ajánlása, hirdetések továbbítása, a fogyasztók vagy kereskedelmi partnerek tájékoztatása, üzletkötés (vásárlás) előmozdítása érdekében.

3.26. **érintett:** bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

3.27. **harmadik személy:** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

3.28. **hozzájárulás:** az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. A hozzájárulás – a különleges adatok kezelésére adott hozzájárulást kivéve – nincs alakszerűséghez kötve, történhet kifejezett nyilatkozattal és ráutaló magatartással is, azonban a hozzájárulásnak minden esetben bizonyíthatónak kell lennie.

3.29. **informatikai eszköz:** bármely feladat ellátására létrehozott, informatikai technológia felhasználásával működtetett (pl. vezérelt) telepített, vagy mobil eszközök, továbbá rendszerek, eljárások összessége vagy ezek alkotó elemei (pl. számítógép, hordozható informatikai eszköz és adattároló, nyomtató, operációs rendszer, felhasználói programok [irodai alkalmazások, adatbáziskezelő, vezérlő programok, beágyazott informatikai rendszerek és egyéb egyedi fejlesztésű célprogramok stb.], továbbá az informatikai alapokra épülő távközlési rendszerek [pl. IP telefon rendszer és végberendezései, hálózati aktív és passzív eszközök], valamint a hálózatmenedzsment elemei).

3.30. **informatikai eszközök ellenőrzésének indokolt esetei különösen:**

- a munkavállaló mobiltelefon használatánál a számára engedélyezett költségkeretet indokolatlanul túllépi,

- a munkavállaló munkaköre gyakorlása során tudomására jutott védendő információt arra illetéktelen személlyel, vagy szervezettel megosztja,
- a munkavállaló munkáltatója felé fennálló együttműködési kötelezettségét megszegve jár el,
- amennyiben az érintett munkavállaló nyilatkozatának beszerzése lehetetlen és azt a közeli hozzátartozója írásban, indokai megjelölésével kéri, továbbá alappal feltehető, hogy az adatok kiadása az érintett munkavállaló létfontosságú érdekei védelméhez szükséges, valamint az adatok kiadását az adatvédelmi kapcsolattartó, szükség szerint a Jogi Igazgatóság véleményének kikérését követően, indokoltnak, az információs önrendelkezési jog korlátozásával arányosnak tartja,
- minden olyan körülmény, amely alapján alappal feltételezhető, hogy a munkavállaló az általában elvárható etikai normák súlyos megszegésével járt el, és azt az adatvédelmi kapcsolattartó is indokoltnak, az információs önrendelkezési jog korlátozásával arányosnak tartja.

3.31. **irat:** valamely szerv működésével, illetve személy tevékenységével kapcsolatban írásban vagy elektronikus úton készített szöveg, számadatsor, vázlat, grafikon és ábra.

3.32. **kötelező adatkezelés:** a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

3.33. **közterület:** a közhasználatra szolgáló olyan állami vagy önkormányzati tulajdonban álló terület, amelyet rendeltetésének megfelelően mindenki korlátozás nélkül igénybe vehet, ideértve a közterületnek közútként szolgáló részét is.

3.34. **különleges adat:** a) a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, vallásos vagy más világnézeti meggyőződésre, érdekképviselési szervezeti tagságra, a szexuális életre vonatkozó személyes adat,

b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűn- ügyi személyes adat.

3.35. **megfelelő tájékoztatás:** az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá 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, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

3.36. **Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH):** Nemzeti Adatvédelmi és Információszabadság Hatóság: Jogállását és feladatait az Info tv. 38.§-a határozza meg (a továbbiakban: Hatóság).

3.37. **nyilvános adat:** minden olyan tény, adat, információ, amelyek bárki számára hozzáférhetők. Személyes adat nyilvánosságáról kizárólag törvény rendelkezhet.

3.38. **nyilvánosságra hozatal:** az adat bárki számára hozzáférhetővé tétele.

3.39. **személyes adat:** az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható, tehát az adatkezelő rendelkezik azokkal a feltételekkel, amelyek a helyreállításhoz szükségesek.

3.40. **személyes adat-gazda:** egy adott szervezeti egységnél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat jelen szabályzatnak megfelelő kezelésért (továbbiakban: adatgazda). Amennyiben IT rendszerben kezelt személyes adattal kapcsolatos döntés meghozatala szükséges, és az érinti az adatgazda felelősségét, akkor a személyes adatgazda a Szabályzat alapján kijelölt vezető egyetértésével hozza meg döntését.

3.41. **profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

3.42. **távolról végzett munka/ távmunka:** a Centrum informatikai rendszerének biztonsági zónáján kívül eső (nem védett) környezetből végzett tevékenység, amely során a Centrum a felhasználó számára olyan informatikai

erőforrások elérését biztosítja (jellemzően VPN-en keresztül), amellyel a munkahelyén egyébként rendelkezhet. Ide nem értendők azoknak a technológiáknak, illetve mobil informatikai megoldásoknak alkalmi felhasználása, amellyel eseti információcserét lehet megvalósítani (pl. OWA, Push email, OAW). E szabályzat alkalmazása során a távról végzett munka tartalmában nem azonos a Munka Törvénykönyvében szabályozott távmunka fogalommal.

3.43. **tiltakozás:** az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

3.44. **munkahelyi azonosítószám:** a Centrum munkavállalóját az adatkezelés során egyértelműen azonosító, belső azonosítási célokat szolgáló számjegysor.

3.45. **VPN:** (Virtual Private Network – virtuális magánhálózat): olyan informatikai hálózat, amely nyilvános kommunikációs csatornák és eszközök segítségével valósul meg, de az azokon zajló egyéb forgalomtól logikailag elkülönülő, mások számára nem hozzáférhető egységet képez. A VPN az adatok védelmére, a hitelesítés mellett, titkosítást is alkalmaz, miáltal lehetőséget biztosít a Centrum számára, hogy a belső hálózat meghatározott elemeit kívülről elérhetővé tegye az erre feljogosított (pl. zárt felhasználói csoport, illetve távmunkát végző) felhasználók számára.

3.46. **zártan kezelendő:** a személyes adatot tartalmazó dokumentumok általános védelmi előírása. Amennyiben az adathordozóról nem állapítható meg egyértelműen adattartalmának védendő jellege, vagy az adatkezelő külön ki kívánja emelni a kezelés zártságának követelményét, abban az esetben ezt kezelési utasításként kell a dokumentumon feltüntetni.

4. A SZEMÉLYES ADATOK KEZELÉSE ÉS VÉDELME

4.1. Alapelvek és alapvető rendelkezések

4.1.1. A Centrumnál személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, továbbá az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.

A Centrum kizárólag olyan személyes adatot kezelhet – a cél megvalósulásához szükséges mértékben és ideig –, amely elengedhetetlen az adatkezelés céljának megvalósulásához és a cél elérésére alkalmas, továbbá személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

4.1.2. A Centrum gondoskodik arról, hogy az adatokhoz csak olyan munkavállalók, adatfeldolgozók férhessenek hozzá, akik vagy amelyek adatkezelése, adatfeldolgozása vonatkozásában a célhoz kötöttség elve megvalósultnak tekinthető.

4.1.3. A célhoz kötöttség elve megvalósulásának vizsgálata minden esetben az illetékes adatgazda feladata és felelőssége. Az adat kiadására – ideértve a Centrum szervezeti egységei közötti adatátadásokat is – vonatkozó kérések esetében az adatkérőnek az adatkérés célját minden esetben meg kell jelölni, az adatszolgáltató pedig köteles mérlegelni, hogy a kért adatok a megjelölt cél eléréséhez elengedhetetlenül szükségesek-e. Az adatkérőnek kizárólag olyan adat adható át, ami a cél eléréséhez elengedhetetlenül szükséges. Amennyiben az adatkezelés célhoz kötöttsége kétséges, az adatgazda köteles a kérdésben a belső adatvédelmi kapcsolattartó állásfoglalását beszerezni.

4.1.4. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha a Centrum rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

4.1.5. Az adatkezelés során a Centrumnak biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

4.2. Az adatkezelés jogalapja

- 4.2.1. Személyes adatot a Centrum – az érintett hozzájárulásán túlmenően – akkor kezelhet, ha
- a) azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés),
 - b) az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése
 - ba) a Centrumra vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
 - bb) a Centrum vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

4.2.2. Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatait a Centrum kezelheti.

4.2.3. A 16. életévét be nem töltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása szükséges.

4.2.4. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, a Centrum a felvett adatokat törvény eltérő rendelkezésének hiányában a 4.2.1. pont b) alpontjában meghatározott esetekben további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

4.2.5. Különleges adatot a Centrum az érintett írásbeli hozzájárulása, törvény elrendelése alapján, illetve a 4.2.1. pont b) alpontjában meghatározott esetekben kezelhet.

4.2.6. Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Amennyiben az érintett a Centrumnál írásban kötött szerződés teljesítése érdekében adja hozzájárulását az adatkezeléshez, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul az adatai szerződésben meghatározottak szerinti kezeléséhez.

4.3. Az érintett előzetes tájékoztatásának követelménye

4.3.1. Az érintettel az adatkezelés megkezdése előtt az adatkezelést végzőnek közölni kell, hogy az adatkezelés hozzájáruláson alapul (önkéntes) vagy kötelező.

4.3.2. Kötelező adatkezelés esetén nem szükséges az érintett hozzájárulásának a beszerzése és nem kell az érintettel adatvédelmi nyilatkozatot aláíratni, mert az adatkezelés jogalapja a törvényi felhatalmazás és nem az érintett hozzájárulása. Ebben az esetben is az érintettet tájékoztatni kell az adatkezelés jogalapjáról, tehát arról, hogy melyik jogszabály felhatalmazása alapján történik a személyes adatainak kezelése.

4.3.3. Az adatkezelés megkezdése előtt az adatkezelést végzőnek az érintettet - kérés nélkül is - előzetesen egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen

- a) az adatkezelés kötelező, vagy hozzájáruláson alapuló voltáról,
- b) az adatkezelés céljáról és jogalapjáról (önkéntes vagy jogszabály által kötelező),
- c) az adatkezelő személyéről, adatfeldolgozás esetén az adatfeldolgozó kilétéről,
- d) az adatkezelés időtartamáról,
- e) az adattovábbítás címzettjeiről,

- f) hozzájárulásos adatfelvétel esetén a Centrum a felvett adatokat törvény eltérő rendelkezése hiányában fa) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
- fb) a Centrum vagy harmadik személy jogos érdekeinek érvényesítése céljából (ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jogok korlátozásával arányban áll) történő kezeléséről és arról, hogy ezek fennállása esetén további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti,
- g) az érintett jogairól: tájékoztatás az adatkezelésről, adatfelvételt követően kérheti adatainak helyesbítését, valamint – a kötelező adatkezelés kivételével – az adatainak törlését vagy zárolását, tiltakozhat a kezelés ellen,
- h) jogorvoslati lehetőségeiről: adatvédelmi hatósághoz, bírósághoz fordulás,
- i) kik ismerhetik meg az adatokat, valamint
- j) a szolgáltatás igénybevétele megghiúsulásáról, ha az ügyfél az ahhoz szükséges személyes adatokat nem adja meg, illetve nem járul hozzá azok kezeléséhez.

4.3.4. Kötelező adatkezelés esetén a tájékoztatás megtörténhet a 4.3.3. pont szerinti információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

4.3.5. Ha az érintett(ek) személyes tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás az alábbi információk nyilvánosságra hozatalával is megtörténhet:

- a) az adatgyűjtés ténye,
- b) az érintettek köre,
- c) az adatgyűjtés célja,
- d) az adatkezelés időtartama,
- e) az adatok megismerésére jogosult lehetséges adatkezelők személye,
- f) az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetése,
- g) az adatkezelés nyilvántartási száma, ha az adatkezelés adatvédelmi nyilvántartásba vételének van helye, kivéve ha a Hatóság a nyilvántartásba vétel iránti kérelmet nem bírálta el.

4.3.6. A 4.3.5. pontban meghatározottak végrehajtásáról az illetékes terület adatgazdája dönt, indokolt esetben a belső adatvédelmi kapcsolattartó álláspontjának beszerzését követően.

4.4. Az adatbiztonság követelménye

4.4.1. A Centrum az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve). Az informatikai rendszerekben megvalósuló adatkezelések során a Centrum mindenkor hatályos jogszabályoknak megfelelően kell alkalmazni minden olyan adatbiztonsági kérdésben, amelyre jelen Szabályzat nem tartalmaz előírást.

4.4.2. A Centrum köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét. A Centrum, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Infotv., és a belső szabályzat, valamint az egyéb adat- és titokvédelmi szabályokban megfogalmazottak érvényre juttatásához szükségesek.

4.4.3. Ennek keretében az adatgazdák az adott szervezeti egység által kezelt személyes adatok tekintetében kötelesek:

- Az adatkezelés időtartama alatt az adatok biztonságos tárolása, az időtartam lejártával az adatállomány törlése, fizikai megsemmisítése érdekében a szükséges intézkedéseket megtenni;
- Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés a véletlen megsemmisítés és sérülés, a Centrum által alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen.

- Gondoskodni arról, hogy a jelen Szabályzatot, valamint a feladatkörükben kiadott külön, a személyes adatok kezeléséről szóló rendelkezéseket az irányításuk alatt dolgozók megismerjék és betartsák, illetve azt folyamatosan ellenőrizni;
- Ellenőrizni, hogy a szervezeti egységében kezelt adatok továbbításukat követően is olyan adatkezelőhöz, adatfeldolgozóhoz kerülnek, aki vagy amely az adatok biztonságos kezeléséről megfelelően gondoskodni tud, ezzel összefüggő kérdésekben jogosult kérni a adatvédelmi kapcsolattartó állásfoglalását;

A Centrum valamennyi munkavállalója köteles a személyes adatokat tartalmazó iratokat és a munkavégzéshez szükséges segédleteket a munkavégzés befejezését követően – ahol biztosított – zárható lemez- vagy páncélszekrényben, biztonsági zárral ellátott fiókban, szekrényben tárolni. Ahol ezek a feltételek nem biztosítottak ott is törekedni kell az adatok legalább zárral ellátott fiókban, szekrényben történő biztonságos tárolására. Az íróasztalokon a munkavégzés befejezését követően személyes adatokat tartalmazó iratok tárolása tilos.

4.4.4. Az adatokat a Centrumnak megfelelő intézkedésekkel védenie kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetlenné válás ellen.

4.4.5. A személyes adatok automatizált feldolgozása során biztosítani kell a jogosulatlan adatbevitel megakadályozását, annak ellenőrizhetőségét, hogy a személyes adatokat mely szerveknek továbbították, a személyes adatokat mikor és ki vitte be az adatfeldolgozó rendszerbe, a telepített rendszerek üzemzavara esetén az adatok helyreállíthatóságát, valamint azt, hogy a fellépő hibákról jelentés készüljön.

4.4.6. Az elektronikusan kezelt adatállományok védelme érdekében a Centrum megfelelő technikai megoldással köteles biztosítani, hogy a különböző nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelkezhetők. A Centrum munkavállalóinak adatai, függetlenül attól, hogy egy közös, vagy osztott adatbázisban szerepelnek, a munkavállaló szempontjából egy nyilvántartásnak tekintendők.

4.4.7. A Centrumnak és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

4.5. Adatfeldolgozás

4.5.1. A Centrum a munkaviszonyból, illetve gazdasági tevékenységének ellátáshoz származó kötelezettségek teljesítése céljából, (számlázáshoz, bérszámfejtéshez szükséges szoftverek) az adatszolgáltatás céljának megjelölésével, a munkavállalók, illetve vásárlók személyes adatait adatfeldolgozó számára átadhatja, amelyről a munkavállalókat előzetesen tájékoztatni kell.

4.5.2. A Centrum határozza meg az általa megbízott adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályi előírások keretei között. Az adatkezelési műveletekre vonatkozó szabályzatok jogszerűségéért és jelen szabályzat előírásainak történő megfeleléséért a Centrum, illetve az adatkezelő szervezet vezetője a felelős.

4.5.3. Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Centrum rendelkezései szerint dolgozhatja fel, és ezek felhasználásával saját céljára adatfeldolgozást nem végezhet, továbbá köteles a személyes adatokat a Centrum rendelkezései szerint tárolni és megőrizni.

4.5.4. A Centrumnak az adatfeldolgozásra vonatkozó szerződéseit írásba kell foglalnia. A szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából releváns, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, az adatfeldolgozás célját, a kezelendő adatok biztonságával kapcsolatos elvárásokat, az adatok kezelésének ellenőrzési lehetőségét. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A szerződés kidolgozása során biztosítani kell az adatvédelmi kapcsolattartó véleményezési jogát.

4.5.5. Az adatfeldolgozó tevékenységének ellátása során további adatfeldolgozót a Centrum rendelkezései alapján vehet igénybe. Amennyiben az adatfeldolgozó további adatfeldolgozót kíván megbízni egyes adatfeldolgozási műveletek elvégzésével, ehhez a Centrum előzetes írásbeli hozzájárulására van szükség. Az adatkezelésben érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet. A szerződés kidolgozása során biztosítani kell az adatvédelmi kapcsolattartó véleményezési jogát.

4.6. Az érintettek jogai és érvényesítésük

4.6.1. A Centrum biztosítani köteles, hogy a munkavállaló a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphasson.

4.6.2. Az érintett az adatkezelést végző szervezeti egység vezetőjénél kérheti a személyes adatai

- kezeléséről történő tájékoztatását;
- helyesbítését, illetve kijavítását;
- törlését, amelyek kezelésére a Centrum nem rendelkezik törvényi felhatalmazással, vagy amely adat kezelése az érintett hozzájárulásának hiányában a továbbiakban nem kezelhető;

Az érintett e kérdésével az adatvédelmi kapcsolattartóhoz is fordulhat.

4.6.3. A Centrumnak az érintett kérelmére legfeljebb 30 napon belül írásban, közérthető formában tájékoztatást kell adnia

- a) az általa kezelt, illetőleg az általa megbízott adatfeldolgozó által feldolgozott adatairól
- b) az adatkezelés
 - adatainak forrásáról
 - céljáról
 - jogalapjáról
 - időtartamáról
- c) az adatfeldolgozó
 - nevéről
 - címéről (székhelyéről)
- d) az adatkezeléssel összefüggő tevékenységéről
- e) adattovábbítás esetén annak jogalapjáról és címzettjéről.

4.6.4. A Centrum köteles a személyes adatot törölni, amennyiben

- a) annak kezelése jogellenes,
- b) az érintett kéri,
- c) az hiányos vagy téves és ez az állapot jogszerűen nem orvosolható – feltéve, hogy a törlést törvény nem zárja ki,
- d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt,
- e) azt bíróság vagy a NAIH elrendelte.

4.6.5. A Centrum törlési kötelezettsége nem vonatkozik azon személyes adataira, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

4.6.6. A Centrum a hibás személyes adatot, amennyiben a valóságnak megfelelő személyes adat a rendelkezésre áll, saját kezdeményezésre, illetve az érintett kérésére, az általa bemutatott dokumentumok alapján helyesbíti, illetve az adatfeldolgozónál helyesbítetteti.

4.6.7. Törlés helyett a Centrum zárolja a személyes adatot, ha ezt az érintett kéri, vagy ha a rendelkezésre álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így zárolt személyes adat kizárólag azon adatkezelési cél fennállásáig kezelhető, amely kizárta a személyes adat törlését.

4.6.8. A Centrum megjelöli az általa kezelt személyes adatot, ha az érintett annak helyességét vagy pontosságát vitatja, de a rendelkezésre álló dokumentumok alapján nem állapítható meg egyértelműen annak helytelensége vagy pontatlansága.

4.6.9. Az adatok törlésről, a helyesbítésről, a zárolásról, a megjelölésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban azt adatkezelés céljára továbbították. Az értesítés abban az esetben mellőzhető, ha az – tekintettel az adatkezelés céljára – nem sérti az érintett jogos érdekét.

4.6.10. A kérelem elutasítása esetén az adatkezelő a kérelem kézhezvételét követő 30 napon belül írásban közli az elutasítás indokait, továbbá tájékoztatja az érintettet a bírósági jogorvoslat, valamint a Hatósághoz fordulás lehetőségéről.

4.7. Az adatkezelésben közreműködők és feladataik

4.7.1. Minőségirányítási vezető

4.7.2. A Centrum minőségirányítási vezetője irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását.

4.7.3. Személyes adatokat kezelő munkavállaló

A Centrum azon munkavállalója, aki személyes adatok kezelésével kapcsolatos tevékenységet végez, köteles gondoskodni arról, hogy

- a) az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások
- b) indokolt esetben a személyes adatot tartalmazó adathordozókon és dokumentumokon a „Zártan kezelendő” kezelési jelölés feltüntetésre kerüljön
- c) az informatikai eszközök adathordozóján tárolt személyes adatok törlése esetén azok a későbbiekben ne legyenek visszaállíthatók
- d) a személyes adat indokolt esetben törlésre, illetve zárolásra kerüljön.
- a) irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet.

5. AZ ADATKEZELÉS RÉSZLETES SZABÁLYAI, A CENTRUM ÁLTAL KEZELT ADATCSOPORTOK

5.1. Adatcsoportok

Személyes adatok a Centrum szervezeti keretein belül a következő csoportokban kezelhetők:

- I. ügyfeladatok, beleértve a Centrum partnereinek ügyfélkapcsolati adatait és a Centrum szolgáltatásait igénybe vevő szerződéses kapcsolatban álló természetes személyek adatait is;
- II. a Centrum munkavállalóinak adatai (beleértve a toborzással kapcsolatban keletkező, nem munkavállalókhöz kapcsolódó adatokat, valamint az érintett munkavállaló kérelmére indult eljárásban);
- III. hatósági adatszolgáltatások;
- IV. belső adatvédelmi nyilvántartás;

V. adattovábbítási nyilvántartás.

6. AZ ÜGYFÉLADATOK KEZELÉSE

6.1. A Centrum által nyújtott gazdasági üzleti tevékenység keretében nyújtott szolgáltatások igénybevételére irányuló vásárlásra vonatkozó jogszabályban kötelezően meghatározott adatok, valamint az érintett természetes személyazonosító adatain kívül kizárólag olyan adatok szerepelhetnek, amelyek a szerződés teljesítése, és az ügyfél tartozásával kapcsolatos követelések érvényesítéséhez, az üzleti kockázat felméréséhez elengedhetetlenül szükségesek.

6.2. Amennyiben az érintett ezen adatokat a szerződéskötés során szolgáltatni nem kívánja, a szerződéskötés megtagadható. Az ezen adatok kezeléséhez adott hozzájárulást meghatározott célra vélelmezni kell. Kétség esetén a szerződéskötéshez kérhető adatok köréről a belső adatvédelmi kapcsolattartó állásfoglalását kell kérni.

6.3. Ha az adatkezelés időtartama alatt az érintett adatainak változását bejelenti, vagy az adatok megváltozását bármely adatkezelő, adatfeldolgozó észleli, az adatokat a változásnak megfelelően haladéktalanul módosítani kell, illetve ki kell egészíteni. Ebben az esetben a módosításra kerülő korábbi, valamint a módosítást, kiegészítést követő új adatokat egyaránt fel kell tüntetni a nyilvántartásban, oly módon azonban, hogy a nyilvántartásból az adatok aktív, illetve inaktív állapota egyértelműen megállapítható legyen.

6.4. Amennyiben a Centrum vagy az érintett ügyfél az igénye érvényesítése iránt eljárást indít, az adatok az egyeztetés folyamán, valamint a bírósági, hatósági eljárás befejezéséig nyilvántarthatók.

6.5. Ha az ügyféli jogviszonyban számla kibocsátására kerül sor, a számlán szereplő adatok a számviteli- és adójogszabályokban meghatározott határidőig tarthatóak nyilván.

A törlésig a Centrum az ügyfelek szerződésben szereplő adatait papír- és elektronikus formában is nyilvántartja.

7. A CENTRUMMAL SZÁLLÍTÓI SZERZŐDÉSES KAPCSOLATBAN ÁLLÓ TERMÉSZETES SZEMÉLYEK ADATAINAK KEZELÉSE, PARTNER-NYILVÁNTARTÁS

7.1. A Centrummal szerződéses kapcsolatban álló természetes személyek (pl. egyéni vállalkozó beszállítók, alvállalkozók) adatainak kezelése során a fenti pontban foglaltakat kell értelemszerűen alkalmazni beleértve az adatvédelmi nyilvántartásba történő bejelentést is, azzal az eltéréssel, hogy ezen szerződések személyes adatállományát az ügyfeladatoktól elkülönítetten kell nyilvántartani (partner nyilvántartás).

8. A MUNKAVÁLLALÓK SZEMÉLYES ADATAINAK KEZELÉSE

8.1. A munkavállalók adatainak kezelése tekintetében az adatgazda a Centrum, továbbá minden olyan szervezeti egység vezetője, akinek az irányítása alatt álló egységnél munkavállalói adatokat kezelnek. A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.

8.2. Amennyiben a munkába lépésre irányuló felvételi eljárást követően munkaviszony létesítésére nem kerülne sor, az érintett adatait haladéktalanul törölni kell, kivéve, ha az érintett írásban hozzájárul ahhoz, hogy az adatait a Centrum továbbra is kezelje. Az így keletkezett személyes adatokat a szervezet kezeli, az érintett írásbeli hozzájárulásában meghatározott ideig.

8.3. A Centrum a személyi nyilvántartásban a munkavállalók következő adatait (együtt: személyi anyag) kezelheti:

- a) a munkavállaló természetes személyazonosító adatait, nemét, lakóhelyét, tartózkodási helyét;
- b) állampolgárságát;
- c) TAJ számát;
- d) adóazonosító jelét;
- e) munkába lépésének kezdő és befejező időpontját;
- f) munkakörét;
- iskolai végzettségét, szakképzettségét, nyelvismeretét, az ezt igazoló okiratok másolatát, a tanulmányi szerződést;
- h) a munkavállaló önéletrajzát;
- i) munkabérének összegét, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatokat;
- j) a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát;
- k) a munkavállaló által a munkaviszony megszűnésének évében igénybe vett betegszabadság időtartamát;
- l) a munkavállaló rendes szabadságával, rendes és rendkívüli munkaidejével, szabadságának kiadásával, egyéb munkaidő-kedvezményével kapcsolatos adatokat;
- m) a munkavállalóval kötött munkaszerződés egyéb lényeges adatait (pl.: a munkavállaló számára biztosított kedvezményeket, a munkavállaló napi/havi munkaidejét, a szerződés fajtáját);
- n) a munkavállaló munkájának értékelését;
- o) a munkavállaló fényképét, kameraképét;
- p) a munkaviszony megszűnésének módját, indokait;
- q) munkakörtől függően erkölcsi bizonyítványát;
- r) a munkaköri alkalmassági vizsgálatok összegzését;
- s) magán nyugdíjpénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezését, azonosító számát és a munkavállaló tagsági számát;
- t) külföldi munkavállaló esetén útlevelszámát; munkavállalási jogosultságot igazoló dokumentumának megnevezését és számát;
- u) minden egyéb olyan személyes adatot, amelynek kezelését törvény írja elő, vagy amelyhez az érintett hozzájárult. Ilyen különösen a családi adókedvezmény igénybe vételéhez szükséges adat, a munkavállaló saját gépjárművének adata, a szociális-jóléti juttatások folyósításához (segély, lakáscélú támogatás, albérleti hozzájárulás), megváltozott munkaképességet, egészségkárosodást, vagy fogyatékosságot igazoló szakhatósági véleményt (ORSZI, OOSZI, NRSZH), vagy fogyatékosságot igazoló szakorvosi aláírással ellátott zárójelentés.

8.4. A Centrum törvény felhatalmazása alapján vagy az érintett hozzájárulására – az erre feladatkörük meghatározásával kijelölt szervezeti egységei útján – kezelheti továbbá a munkavállalók következő adatait is, így különösen:

- a) munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat;
- b) a Centrumnál biztonsági és vagyonvédelmi célból alkalmazott kamerarendszerek által rögzített adatokat.

8.5. Az adott szakterületnél már rendelkezésre álló személyes adatok (többszöri, nem frissítés célú) újrakérése tilos. Az adatok ismételt megadásának megtagadása miatt a munkavállalót semmiféle hátrány nem érheti. A Centrum a munkavállaló egyéb személyes adatait kizárólag az érintett – írásbeli - hozzájárulásával kezelheti. A munkavállalók személyi anyagával kapcsolatos nyilvántartást meghaladó mértékű adatkezelésre csak a munkavállaló hozzájárulásával kerülhet sor.

8.6. A munkaviszony létesítésére szolgáló eljárás keretében, a munkavállaló közreműködése nélkül, kizárólag a nyilvánosság számára, az érintett által korlátozás nélkül (pl. internet, sajtó) hozzáférhetővé tett információ használható fel, ideértve az érintett által kifejezetten a munkavállalásának elősegítése érdekében közzétett (pl. Facebook.com szociális háló útján rögzített) adatot. Harmadik személytől a munkáltató csak a munkavállaló előzetes hozzájárulásával kérheti rá vonatkozó személyes adat szolgáltatását.

8.7. Az érintett kifejezett hozzájárulása, illetve jogszabályi előírás hiányában, a munkaviszony létesítésének meghiúsulása esetén, a felvételi eljárás során rögzített személyes adatokat 30 munkanapon belül törölni kell.

8.8. A munkavállaló adatait a következő személyek ismerhetik meg:

- az érintett (kamerakép esetén az adott kameraképen szereplő érintettek);
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig a Centrum könyvelés vezetője, illetve meghatározott – az érintett személyi anyagát kezelő – alkalmazottja;
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig az érintett munkahelyi vezetői (a munkáltatói jogkörgyakorló vezetővel bezárólag) és az általa kijelölt munkatársai;
- konkrét ellenőrzés céljából az ahhoz elengedhetetlenül szükséges esetben, mértékben és ideig a adatvédelmi kapcsolattartó, az ügyvezető, valamint a vizsgálati jogkörrel felruházott szervek munkatársai;
- bíróság, ügyészség, nyomozó hatóság, illetve más eljáró hatóság hivatalos megkeresés alapján az igényelt mértékig;
- más személyek – indokolt esetben – az érintett írásos hozzájárulásával, a hozzájárulás mértékéig.

8.9. A munkaviszony megszűnését követő 10 év elteltével a munkavállaló adatait törölni kell személyi nyilvántartásból az illetékes szervezetnek, illetve annak a szervezeti egységnek, amelynek a személyzeti nyilvántartásban a munkavállaló adata szerepel kivéve, ha a Centrum és a munkavállaló között ettől eltérő időtartalmú írásbeli megállapodás jön létre. A törlés az írásbeli megállapodásban nem szereplő munkavállalói adatokra terjed ki.

8.10. Nem kell, illetve nem szabad törölni a munkaviszony megszűnését követően sem a munkavállaló azon adatait, amelyek törvény felhatalmazása alapján a továbbiakban is nyilvántarthatók vagy megőrzendők.

8.11. Humán Információs rendszer (SAP, KIRA) útján történő adatkezelés

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

A Centrum a rendszerben, valamint a személyügyi dossziében elhelyezett adatok nyilvántartásának vezetéséhez az érintett munkavállaló saját magára vonatkozóan köteles adatot szolgáltatni. A nyilvántartás pontossága, teljessége, naprakészsége érdekében az érintett munkavállaló az adatkörében beállt változásról köteles öt munkanapon belül, írásban bejelentést tenni.

Az alkalmazott törzsszám a rendszer által generált olyan belső azonosító, amely nem tartalmaz az érintett munkavállalóval kapcsolatba hozható személyes adatot. Használata a munkaviszonnyal közvetlenül összefüggő, az e státuszhoz kapcsolódó adatkezeléseknél megengedett.

A munkavállalók humán adataihoz történő belépési-, betekintési- és hozzáférési jogosultságokat munkakörhöz igazítottan, a munkavégzés megfelelő ellátásához szükséges legkisebb mértékű jogosultsági szinten kell meghatározni. Az adatokhoz történő hozzáférést, az azokkal végzett műveleteket – a rendszer lehetőségeihez mérten – részletesen naplózni kell. A közvetlen munkahelyi vezetők felelősségi körébe tartozik a jogosultságok fentiek szerint meghatározott legkisebb mértékű használatának biztosítása és a hatáskörtúllépés kizárása, ennek ellenőrzése, naprakészségének biztosítása, a jogosultságok beállításának, módosításának, visszavonásának kezdeményezése.

8.12. Jelentési és tájékoztatási kötelezettség

Az a munkavállaló, akinek tudomására jut, hogy a Centrum, vagy annak adatfeldolgozója által kezelt személyes adat jogosulatlan személy tudomására jutott, vagy jogsértő módon került továbbításra, köteles erről a Centrum adatvédelmi kapcsolattartóját tájékoztatni. Az adatvédelmi kapcsolattartója intézkedik az eset körülményeinek feltárásáról és az adatkezelő szerv vezetőjén keresztül gondoskodik az érintett haladéktalan tájékoztatásáról.

8.13. A személyes adatok védelme adatfeldolgozó igénybevétele esetén

A Centrum a munkaviszonyból származó kötelezettség teljesítése céljából a munkavállaló személyes adatait adatfeldolgozó számára átadhatja, amelyről a munkavállalót előzetesen tájékoztatni szükséges.

A munkavállalót már a belépéskor tájékoztatni kell adatainak külső szolgáltatóhoz történő továbbításáról. Ezt közérthetően és olyan módon kell megfogalmazni, hogy abból a munkavállaló számára világos legyen, hogy mely személyi kör jogosult az adataihoz hozzáférni.

A szolgáltató számára szerződésben kell meghatározni, hogy az adatok védelme érdekében milyen intézkedéseket kell megtennie, illetve a védendő adatok megőrzésére, valamint annak megszegése jogkövetkezményeire vonatkozó előírásokat is meg kell fogalmazni, tekintve, hogy az adatfeldolgozó által okozott, a munkavállalót ért kárért a munkáltató köteles helytállni.

8.14. A munkavállaló ellenőrzése

8.14.1. A Mt. lehetőséget biztosít arra, hogy a munkáltató a munkavállalót a munkaviszony rendeltetésével közvetlenül összefüggő, feltétlenül szükséges okból ellenőrizze. A végrehajtás módját egyértelműen, érthetően és pontosan kell meghatározni, beleértve a megfigyelés érdekében alkalmazott eszközökkel kapcsolatos részletszabályokat, a munkavállaló személyes adatai, személyiségi jogai védelmének garanciáit is, betartva a célhoz kötöttség és a tisztességes adatkezelés elvét. A megfigyelőrendszer elsődlegesen az emberi élet, testi épség, a személyi szabadság védelme, veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírok védelme, vagyonvédelem céljából lehet alkalmazni.

8.14.2. A munkavállaló kizárólag a munkaviszonnyal összefüggő magatartása tekintetében ellenőrizhető, amely nem járhat a személyes adatai, személyiségi jogai, az emberi méltósága megsértésével. A munkavállalót előzetesen tájékoztatni kell azoknak a technikai eszközöknek az alkalmazásáról, amelyek az ellenőrzésére szolgálnak.

8.14.3. Kamerás megfigyelés esetén a kamerát nem lehet kizárólag egy munkavállaló, illetve az általa végzett tevékenység megfigyelése céljából elhelyezni, tilos továbbá öltözőkben, zuhanyzóban, illemhelyiségekben, orvosi szobákban, várókban használni.

8.14.4. Az adatkezelőnek minden egyes elektronikus megfigyelő eszköz vonatkozásában pontosan meg kell jelölnie, hogy milyen célból helyezte el az adott területen, milyen területre, berendezésre irányul. A felvételek rögzítése esetén főszabályként azokat három napig lehet megőrizni. Az eszközre vonatkozó helyi adatkezelési szabályzatban kell rögzíteni – többek között – azokat a szabályokat, hogy ki, milyen célból és milyen időközönként nézheti vissza a felvételeket. A visszanezésére kizárólag a Centrumon belül az érintett munkáltatói jogkörgyakorló, az általa megbízott munkavállaló, valamint a belső szabályzatok által kijelölt szakértők számára szabad jogosultságot biztosítani.

8.14.5. Az elektronikus megfigyelőrendszer alkalmazásához nem szükséges a munkavállalók hozzájárulása, azonban előzetesen – igazolható módon – tájékoztatni kell őket a megfigyelőrendszer alkalmazásával együtt járó adatkezelés lényeges körülményeiről, a kamerák látókörében figyelemfelhívó jelzést is el kell helyezni.

A munkáltatónak az alkalmazott eszközökkel kapcsolatos részletszabályokat a belső normatív utasításban kell egyértelműen, érthetően, pontosan, részletesen meghatározni, amelynek kidolgozása során különös tekintettel kell lennie az arányosság követelményére valamennyi adatkezelési cél tekintetében.

8.14.6. Az elektronikus megfigyelőrendszer telepítésekor az alábbi garanciális követelményeket kell megtartani:

1. A munkáltatói ellenőrzés akkor tekinthető jogszerűnek, ha az a munkaviszony rendeltetésével közvetlenül összefüggő okból feltétlenül szükséges.
2. A munkavállaló magánélete nem ellenőrizhető.
3. A munkáltatói ellenőrzés és az annak során alkalmazott eszközök, módszerek nem járhatnak az személyes adatai, személyiségi jogai, emberi méltósága megsértésével.
4. A munkavállalót előzetesen tájékoztatni kell az adatkezelés lényeges követelményeiről.
5. Az adatkezelés akkor jogszerű, ha a munkáltató az adatkezeléssel kapcsolatban betartja az Infotv. alapvető rendelkezéseit, a célhoz kötöttség és a tisztességes adatkezelés elvét.

8.14.7. A munkáltatói ellenőrzés esetleges jogszerűtlensége megalapozhatja a munkavállaló által gyakorolt azonnali hatályú felmondás jogát.

8.14.8. A munkavállaló a munkahelyi ellenőrzésére vonatkozó adatkezelési szabályok megsértése miatt a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat. A Hatóság a megállapított jogellenes adatkezelés, jogsértés súlyától függő bírságot szabhat ki a munkáltatóra.

Amennyiben az esetleges jogszerűtlen munkáltatói ellenőrzés a munkavállaló személyiségi- vagy adatkezeléssel kapcsolatos jogainak sérelmével jár, az érintett a munkáltatótól a polgári jog szabályai szerint sérelemdíjat követelhet, és kérheti a jogellenes adatkezeléssel okozott kára megtérítését.

8.15. Az informatikai eszközök használata, naplózása, ellenőrzése

8.15.1. A Centrum a munkavállalók részére a munkakörök ellátásához, kizárólag munkavégzés céljára asztali számítógépet, hordozható informatikai eszközt, központi tárhelyet, internet-hozzáférést, elektronikus postafiókot biztosíthat. Az informatikai biztonság szintjének fenntartása érdekében ezen eszközök és szolgáltatások használatával kapcsolatos forgalmi adatokat a Centrum a Mt. 11. § (1) bekezdése alapján naplózza és ellenőrzi.

8.15.2. Az ellenőrzésre szolgáló technikai eszközök és biztonsági rendszerek alkalmazásáról a munkavállalókat minden részletre kiterjedően tájékoztatni kell. Az információvédelmi nyilatkozat egyesítve tartalmazza az informatikai biztonságra, a védendő információkra, valamint az adatvédelemre vonatkozó részeket, amelynek egy aláírt példányát a munkavállaló humán dokumentumai között kell elhelyezni.

8.15.3. Az informatikai eszközök és szolgáltatások rendeltetésszerű használatára fel kell hívni a munkavállalók figyelmét, beleértve azt is, hogy az informatikai eszköz használata önmagában megteremti annak jogalapját, hogy az abban rögzített adatokat a munkáltató, a jogszabályi előírásoknak és jelen szabályzatnak megfelelően felhasználja, és az informatikai eszköz használatát ellenőrizze.

8.15.4. Az előírások megsértése esetén, indokolt esetben tájékoztatni kell a munkáltatói jogokat gyakorló vezetőt, aki az adatvédelmi kapcsolattartó és az illetékes rendszergazda bevonásával külön eseti ellenőrzést rendelhet el. Amennyiben az informatikai biztonság veszélyeztetése is felmerül, akkor indokolt az Információvédelem szervezet bevonása. A vizsgálat során biztosítani kell a munkavállaló részvételének lehetőségét. Az ellenőrzés tényét, helyét, indokát, eredményét, valamint a résztvevők nevét jegyzőkönyvben kell rögzíteni.

8.16. Megkeresés alapján történő adattovábbítás

8.16.1. A Centrumhoz külső szervezettől, illetve magánszemélytől érkező, személyes adat kiadására irányuló megkeresés csak akkor teljesíthető, ha az érintett erre írásban felhatalmazza a Centrumot. Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére. Az ilyen megkeresések alapján teljesített adatszolgáltatással kapcsolatos tényeket, körülményeket meghatározott módon dokumentálni kell.

8.16.2. Az adatközlést az érintett nyilatkozattételétől függetlenül teljesíteni kell, ha azt jogszabály írja elő, így különösen büntető ügyekben eljáró hatóságoktól – rendőrség, bíróság, ügyészség, TEK, NAV stb. – valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket. E szervezetek megkereséseiről, amennyiben ennek egyéb törvényi akadálya nincs – az elrendelt nemzetbiztonsági ellenőrzések lefolytatása során történő iratbetekintések, adatkérések kivételével – az illetékes adatkezelő közvetlenül, vagy felettese útján köteles a jegyzőkönyv megküldésével tájékoztatni biztonsági főigazgatót, akinek jóváhagyását követően kell az adatszolgáltatást a meghatározott határidőn belül teljesíteni.

8.17. Elektronikus megfigyelőrendszer (kamerarendszer)

8.17.1. Elektronikus megfigyelőrendszer törvény, illetve helyi önkormányzati rendelet alapján működtethető, továbbá a működés jogalapját az érintett önkéntes hozzájárulása is megteremtheti. A Centrum vonatkozásában a megfigyelés törvényi alapját a vagyonvédelmi tv. biztosítja, egyéb esetekben az Infotv. előírásai irányadók. A felvételeket készítő rendszerek üzemeltetését, mint adatkezelést az adatvédelmi nyilvántartásba be kell jelenteni.

8.17.2. Az elektronikus megfigyelő rendszernek felvételt is lehetővé tevő formája a következő esetekben alkalmazható:

- a) az emberi élet
- b) a testi épség, a személyi szabadság védelme
- c) a veszélyes anyagok őrzése
- d) az üzleti, bank- és értékpapírtitok védelme, valamint
- e) a vagyonvédelem érdekében.

8.17.3. A kamera használata során fennálló körülményeknek valószínűsíteniük kell, hogy a jogsértések észlelése, az elkövető tettenérése, illetve e jogsértő cselekmények megelőzése, azok bizonyítása más módszerrel nem érhető

el, továbbá e technikai eszközök alkalmazása elengedhetetlenül szükséges mértékű, és az információs önrendelkezési jog aránytalan korlátozásával nem jár.

A felvételt felhasználás hiányában legfeljebb a rögzítéstől számított harminc nap elteltével meg kell semmisíteni, illetve törölni kell, ha a rögzítésre

- a) nyilvános rendezvényen az emberi élet, testi épség, személyi szabadság védelme,
- b) a Büntető Törvénykönyvről szóló törvény szerint legalább jelentős értékű pénz, értékpapír, nemesfém, drágakő biztonságos tárolása, kezelése, szállítása érdekében kerül sor.

8.17.4. Felhasználásnak az minősül, ha a felvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

8.17.5. Az, akinek jogát vagy jogos érdekét a felvétel, illetve más személyes adatának rögzítése érinti, az adatkezelés tartamán belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje. Bíróság vagy más hatóság megkeresésére a felvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a felvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

8.17.6. A felvételt, valamint más személyes adatot csak az arra jogosult személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen. A felvételt, valamint személyes adatot kezelő, vagy egyéb okból annak megismerésére jogosult személy- és vagyonvédelmi tevékenységet végző személy nevét, az adatok megismerésének okát és idejét jegyzőkönyvben kell rögzíteni.

8.17.7. Vásárlók számára megnyitott területeken, illetve üzemi területeken, munkaterületeken figyelemfelhívó jelzést, ismertetést kell elhelyezni a megfigyelt területen, jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon. Az adatkezelés önkéntes hozzájárulás alapján történik, amelyet az érintettek tájékoztatáson alapuló ráutaló magatartása alapoz meg.

8.18. A személyes adatokat tartalmazó iratok, adathordozók kezelése

8.18.1. A személyes adatokat tartalmazó iratok, adathordozók kizárólag zárt borítékban (vagy egyéb, ezzel egyenértékű megoldással, pl. számkódos táska) továbbíthatók a címzett részére, és azokon fel kell tüntetni, hogy az „Zártan kezelendő!” Ezt a megjelölést a személyes adatok elektronikus adattovábbítása, valamint elektronikus megjelenítése során is alkalmazni kell. Kivételt képeznek azok az elektronikus adattovábbítások, melyek tartalmi és formai elemeit jogszabály, vagy jogszabály felhatalmazása alapján hatóság írja elő, valamint a humán szolgáltatás belső szervezeti egységei közötti adattovábbítás, amennyiben megfelelően biztosított a munkavállalói személyes adatok illetéktelen hozzáférés elleni védelme.

8.18.2. Az így jelölt adattartalom esetében gondoskodni kell az adatok védett kezeléséről oly módon, hogy azokhoz kizárólag a megismerési jogosultsággal rendelkezők, dokumentált módon férhessenek hozzá – elektronikus feldolgozás, továbbítás esetén, a rendelkezésre álló lehetőségek felhasználásával – technikai védelemmel (pl. a Centrum által rendszeresített titkosítási módszerrel) is biztosítani kell. A kezelési jelölést a dokumentumon és a személyes adatok feldolgozására használt alkalmazások segítségével a számítógépek monitorán is meg kell jeleníteni. Az adatok az érintett életében csak akkor hozhatók nyilvánosságra, ha azt törvény elrendeli, vagy ahhoz az érintett hozzájárult.

8.19. Tiltakozás személyes adat kezelése ellen

Az érintett tiltakozhat személyes adatának kezelése ellen,

- a) ha a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetét;
- b) ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- c) törvényben meghatározott egyéb esetekben.

Az adatkezelő a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

8.20. Bírósági jogérvényesítés

Az érintett jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. Azt, hogy az adatkezelés a jogszabályokban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.

9. A CENTRUM HONLAPJA

9.1. A Centrum honlapján lehetőség van hírlevél szolgáltatás igénybevételére, vagy más értesítésre történő feliratkozásra, amely során név, cégnév és elérhetőségi adatok (e-mail cím, telefonszám stb.) kerülnek rögzítésre. A regisztrációs adatok kizárólag a szolgáltatással kapcsolatosan használhatóak fel, harmadik fél részére nem adhatók át. A szolgáltatás felmondására minden esetben lehetőséget kell biztosítani, amely során a korábban felvett adatokat visszaállíthatatlanul törölni kell. A honlapon hivatkozást kell elhelyezni, amely tartalmazza a honlap adatkezelésére vonatkozó „Adatkezelési tájékoztató”-t és/vagy „Adatkezelési szabályzat”-ot.

9.2. A honlapon korábban elhelyezett nyilatkozatokat a honlap tartalmáért felelős szervezetnek naprakészen kell tartania. Az utolsó változat aktualizálásának időpontját fel kell tüntetni. A szabályozásban bekövetkezett változásról a hírlevélre feliratkozottakat tájékoztatni szükséges.

9.3. A Centrum honlapját látogatók számítógépén cookie elhelyezéséről

9.3.1. Az elektronikus hírközlésről szóló törvény szabályozza a cookie (a továbbiakban: süti) használatát, amely alapján a felhasználó elektronikus hírközlő végberendezésén csak az érintett világos és teljes körű – az adatkezelés céljára is kiterjedő – tájékoztatását követő kifejezett hozzájárulása alapján lehet adatot tárolni, vagy az ott tárolt adathoz hozzáférni.

9.3.2. A felhasználót a jogi közlemény és adatkezelési tájékoztató útján előzetesen teljes körűen és részletesen tájékoztatni kell a számítógépére felmásolni kívánt adatokról, majd miután ehhez megfelelően dokumentált hozzájárulását adta, tölthető fel a süti az eszközére. A süti elhelyezőjének bizonyítani kell tudnia, hogy a felhasználó a hozzájárulását megadta.

9.3.3. A Centrum honlapján a sütik kezelését e szabályoknak megfelelően kell kialakítani, és azokat az adatkezelési nyilatkozat megfelelően dokumentált elfogadását követően lehet a felhasználó végberendezésén elhelyezni.

10. FÉNYKÉP- VIDEO-, HANGFELVÉTEL KÉSZÍTÉS ÁLTALÁNOS SZABÁLYAI

10.1. Adott személyekről készített fénykép- video-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához – törvényi felhatalmazás eseteit kivéve – az érintett személy hozzájárulása szükséges.

10.1.1. A hozzájárulás ráutaló magatartással is megadható, azonban célszerű ehhez írásbeli hozzájárulást kérni. Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összehatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az érintett felismerhető-e.

11. HATÓSÁGI ADATSZOLGÁLTATÁSOK

11.1. A hivatalos szervektől – bíróság, közigazgatási szerv – érkezett, személyes adatokat érintő adatszolgáltatást az illetékes szervezeti egység a megkeresésben megadott határidőig, ennek hiányában 15 napon belül teljesíti, a Centrum általi adatszolgáltatás folyamatáról szóló mindenkori hatályos szabályozásban foglaltaknak megfelelően.

11.2. A nyomozó hatósági adatkéréseket a hatósági adatkérésben illetékes szervezet munkavállalója teljesíti.

11.3. Ha a megkeresés alakiséga, a megkereséssel érintett adatkör kiadhatósága aggályos, az illetékes szervezeti egység a belső adatvédelmi kapcsolattartó soron kívüli állásfoglalását kéri.

11.4. Ha a megkeresés jogszerűségét a belső adatvédelmi kapcsolattartó is aggályosnak tartja, köteles az ügyben a Hatóság sürgősségi eljárását kezdeményezni.

11.5. A megkeresés ez esetben a Hatóság állásfoglalásától függően teljesíthető, kivéve, ha az állásfoglalás a megkeresésben megadott határidő alatt nem érkezik meg a Centrum részére. Ez esetben a megkeresést a megadott határidőben a Centrum kijelölt szervezeti egysége teljesíti.

12. BELSŐ ADATVÉDELMI NYILVÁNTARTÁS

12.1. Az adatkezelést végző szervezeti egység vezetője nyilvántartásba vétel céljából köteles a Centrum adatvédelmi kapcsolattartójának bejelenteni az adatkezelésre vonatkozó adatokat, továbbá az adatkezelésre vonatkozóan helyi adatvédelmi és adatkezelési szabályozást ad ki, amely az adatkezelésre vonatkozó bejelentésben szereplő adatokon túlmenően tartalmazza az adatokhoz hozzáféréssel rendelkezők körét, valamint az adatok elektronikus feldolgozása esetén az adatok mentésének, azok tárolásának rendjét is.

12.2. Az adatkezelésről szóló bejelentést, valamint a helyi adatvédelmi és adatkezelési szabályozást az adatkezelés megkezdését megelőzően legalább 15 nappal meg kell küldeni az adatvédelmi felelősnek a nyilvántartás napra készen történő tartása céljából.

12.3. Meglévő adatkezelésből történő legyűjtés eredményeként létrejövő adatkezelés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül megfogalmazásra, vagy az adatkezelő személye megváltozik. Ilyen esetben erre vonatkozóan is bejelentési, illetve szabályzatkészítési kötelezettség lép életbe. Vitás esetben az adatvédelmi szakértő állásfoglalását kell kérni.

12.4. Az adatvédelmi kapcsolattartó – a belső adatvédelmi nyilvántartás adatai alapján – a személyes adatkezelés nyilvántartásba vételét kéri a NAIH-tól az adatkezelés megkezdése előtt legalább 10 nappal. Az adatkezelés – a kötelező adatkezelés kivételével, illetve amennyiben a NAIH a nyilvántartásba vétel iránti kérelmet a határidőn belül nem bírálja el – a nyilvántartásba vétel nélkül nem kezdhető meg.

12.5. A NAIH számára nem kell bejelenteni – többek között – azt az adatkezelést, amely

- a) az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek adatait tartalmazza;
- b) a foglalkozás-egészségügyi ellátásban kezelt személy betegségére, egészségi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés, vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;
- c) az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik.

12.6. A belső adatvédelmi nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője nyolc napon belül köteles bejelenteni a Centrum adatvédelmi kapcsolattartójának, aki ennek megfelelően módosítja a belső adatvédelmi nyilvántartás adatait, és ha szükséges, kezdeményezi a NAIH szerinti bejegyzés módosítását.

13. ADATTOVÁBBÍTÁSI NYILVÁNTARTÁS

13.1. A Centrum adattovábbítást végző adatkezelőinek nyilvántartást kell vezetnie az általuk végrehajtott adattovábbítások jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából, amelynek tartalmaznia

kell a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását. A nyilvántartás papír alapon, és elektronikus úton is vezethető.

13.2. A felállított adattovábbítási nyilvántartásról, annak papír alapú, vagy elektronikus jellegéről az adatvédelmi kapcsolattartót tájékoztatni kell. A tájékoztatás tartalmazza a létrehozás idejét, helyét, kezelőjét stb. Nem szükséges külön adattovábbítási nyilvántartás készítése amennyiben az adatok a rendszerből lekérdezés útján egyértelműen kimutathatók. A nyilvántartásban az adatokat öt évig, különleges adatok esetében húsz évig meg kell őrizni.

13.3. Adattovábbítás

13.3.1. Adattovábbítás harmadik személy részére

Személyes adatot továbbítani harmadik személy részére csak törvény alapján, vagy az érintett hozzájárulásával lehet, ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Az adatfeldolgozásra irányuló adatátadás nem minősül adattovábbításnak. Az adattovábbítást megelőzően az adatgazda kötelessége megvizsgálni, hogy annak törvényi feltételei fennállnak-e, illetve a továbbítást követően az adatkezelés feltételei minden egyes személyes adatra megvalósulnak-e.

Ugyanazon adatkezelők számára történő, azonos érintettre vonatkozó, és azonos célú adattovábbítás előtt az adatvédelmi kapcsolattartót is be kell vonni a folyamatba. Az ezt követő adattovábbítások során külön vizsgálatot lefolytatni nem kell.

Az adattovábbításról a jelen Szabályzat 5. számú minta szerinti formában adattovábbítási nyilvántartást köteles az adott szervezeti egység vezetni, amelynek egy példányát a tárgyévét követő év január 15-éig az irattárban kell elhelyezni. Az adattovábbítási nyilvántartást az adatátvétel, illetve az adattovábbítás évét követő ötödik év végéig (különleges adatok esetén húsz évig) kell megőrizni.

Az adattovábbítási nyilvántartás tartalmazza:

- a) az adattovábbító által kezelt/gyűjtött személyes adatok továbbításának időpontját,
- b) a továbbított adatköröket,
- c) az adattovábbítás jogalapját és címzettjét (név, cím, székhely),
- d) az adattovábbításért felelős nevét és telefonszámát.

14. A TÁVOLRÓL VÉGZETT MUNKA/ TÁVMUNKA

Amennyiben a munkafeladatok ellátása távolról végzett munka útján valósul meg (pl. VPN kapcsolaton keresztül), és az nem a Centrum által biztosított eszköz igénybevételel történik, a Centrum nem tekinthet be az eszközön tárolt, nem a munkaviszonnyal összefüggő adatokba. Amennyiben a távmunkához a Centrum kizárólag munkavégzés céljára biztosítja az eszközt, a felhasználásával összefüggő tilalom, vagy korlátozás betartásának ellenőrzése céljából a Centrum a teljes adattartalmat ellenőrizheti.

15. A MUNKAHELYI TELEFONHASZNÁLAT ELLENŐRZÉSE

15.1. A munkáltató jogosult a munkavállaló rendelkezésére bocsátott telefon használatát ellenőrizni, amelynek azonban meg kell felelnie az adatvédelmi jogszabályok által támasztott követelményeknek.

15.2. A munkavállaló által lefolytatott telefonbeszélgetések mind a hívott, mind a hívó fél személyes adatának minősülnek, ezért magánjellegű telefonhívásokkal kapcsolatos személyes adatok kezeléséhez mindkét fél hozzájáruló nyilatkozata szükséges. A hivatalos hívásokkal kapcsolatos adatok kezeléséhez nem feltétel az érintett munkavállaló hozzájáruló nyilatkozatának megléte, azonban a tájékoztatás ebben az esetben sem maradhat el.

15.3. A munkáltató, illetőleg az ellenőrzésre feljogosított személy a nem munkavállaló személy hozzájáruló nyilatkozata beszerzésének nehézkes volta, illetve annak lehetetlensége miatt a munkavállaló által lefolytatott magánjellegű telefonhívások adatait nem jogosult kezelni. A célhoz kötött adatkezelés elve megfelelően alátámasztható célt igényelne a munkáltató oldaláról, ami azonban – tekintettel arra, hogy annak megállapításán túl, hogy a munkavállaló telefonhasználatából mekkora összeget tesz ki a magáncélú hívások aránya, további jogosítványa munkáltatói jogosítványokból nem származik – nem igazolható.

15.4. A munkahelyi telefonhasználat ellenőrzésére az alábbi módszerek alkalmazhatók:

- Keretösszeg határozható meg, amely fedezi az adott munkakör betöltéséhez szükséges telefonköltséget. Abban az esetben, ha a munkavállaló e költségen belül maradva, magáncélú telefonbeszélgetéseket is folytat, azt a munkáltató természetbeni juttatásként biztosíthatja részére. A meghatározott költségen felüli összeg a munkavállalóra áthárítható.
- A munkavállaló által használt telefon híváslistája a munkavállalónak lezárt borítékban átadható (azt előzetesen a munkáltató nem kezelheti), amelyről érintett a magán hívások telefonszámaikat oly módon törli, hogy azokat a későbbiekben ne lehessen azonosítani. Az ilyen hívások költségei kiterhelhetők a munkavállalóra.

15.5. A telefonbeszélgetések lehallgatása tilos.

16. AZ INTERNET HASZNÁLATÁNAK ELLENŐRZÉS

16.1. A Centrum az internet hozzáférést bocsájt bizonyos munkavállaló rendelkezésére, annak magán célból történő felhasználását megengedi.

16.2. A Centrum jogosult az internet használatának korlátozására oly módon, hogy megnyitható oldalak körét meghatározza, illetve egyes oldalak megnyitását az informatikai rendszer segítségével korlátozza.

16.3. Amennyiben a kellően tájékoztatott felhasználó annak tudatában keres fel egy honlapot, hogy arról tudomást szerezhetnek, akkor egyúttal hozzájárul ahhoz is, hogy az ellenőrzést lefolytató személy megismerhesse az általa megtekintett oldalakat is.

17. TISZTA ÍRÓASZTAL ÉS TISZTA KÉPERNYŐ

17.1. A személyes adatok megfelelő kezelése érdekében a Centrum valamennyi munkavállalója köteles a papír alapú dokumentumok és a digitális adathordozók fizikai hozzáférés védelméről gondoskodni, amelynek betartását a munkahelyi vezető alkalomszerűen ellenőrzi.

17.2. Tiszta asztal

- a) A személyes adatokat tartalmazó papír alapú, valamint számítógépes adathordozók, hordozható számítógépek illetéktelen személy számára hozzáférhető módon, felügyelet nélkül nem hagyhatók.
- b) Ahol zárható széfek, iratszekrények, fiókok, szekrények nem állnak rendelkezésre, a felügyelet nélkül hagyott iroda ajtaját minden esetben be kell zárni, oda illetéktelen személy bejutását egyéb technikai és szervezési intézkedésekkel meg kell akadályozni.
- c) A munkaidő végén valamennyi személyes adatot tartalmazó adathordozót el kell zárni (pl. széf, lemezszekrény, egyéb zárható bútor), vagy megfelelő technikai intézkedéssel meg kell akadályozni az illetéktelen személy számára az adathoz való hozzáférést, valamint az azt hordozó eszköz eltulajdonítását (pl. Kensington zár).
- d) Személyes adatot tartalmazó információ nyomtatása során a nyomtató nem hagyható őrizetlenül. Technikai akadály esetén gondoskodni kell arról, hogy a később kinyomtatásra kerülő dokumentum ne juthasson illetéktelen kezekbe.

- e) A személyes adatok tárolására, elhelyezésre, feldolgozására szolgáló irodahelyiséget még ideiglenes felügyelet nélkül hagyás esetén is be kell zárni.
- f) A személyazonosító információkat (pl. telefonjegyzék, címjegyzék) oly módon kell elhelyezni, hogy azok tartalmát illetéktelenek ne ismerhessék meg.

17.3. Tiszta képernyő

- a) A személyes adatokat tartalmazó számítógép felhasználója a munkaszoba elhagyása esetén jelentkezzon ki a számítógépéből, vagy zárja azt a „Windows” valamint az „L” billentyű egyidejű lenyomásával.
- b) A személyes adatok feldolgozására alkalmazott számítógép képernyőjét az alábbi módszerek valamelyikének alkalmazásával védeni szükséges a jogosulatlan rálátás, betekintés elől:
 - a munkaasztalok megfelelő elhelyezésével, elfordításával
 - paraván alkalmazásával
 - a helyiségbe történő belépés korlátozásával
 - olyan technikai eszköz felszerelésével, ami a betekintési szöveget jelentősen korlátozza
 - a betekintés ideiglenes korlátozására az a) pontban leírt módszer is alkalmazható.
- c) Amennyiben ezen módszerekkel nem akadályozható meg a betekintés, illetve a helyiségbe rendszeres munkavégzésre beosztott más munkavállaló illetéktelen betekintése, abban az esetben az adatvédelmi szabályok megismertetésével, szükség esetén titoktartási nyilatkozat kitöltésével kell biztosítani az adatok megfelelő védelmét.

A személyes adatok feldolgozására szolgáló alkalmazásokat úgy kell kialakítani, hogy a monitoron történő megjelenítés során figyelmeztető jelzés utaljon a tartalom zárt kezelést igénylő jellegére (pl. figyelmeztető felirattal vagy figyelemfelkeltő szín, effektus használatával). A jelenleg használt alkalmazások korrekciója során gondoskodni kell az előzőekben írtak szerinti megoldás megvalósításáról.

18. ELEKTRONIKUS LEVELEZÉS

18.1. Az elektronikus levelet azonos szintű védelemben kell részesíteni, mint a hagyományos, postai úton továbbított küldeményt. A munkáltató megbízásából, a munkavállaló által hivatalos ügyekben írt és fogadott elektronikus dokumentum tartalmát a munkáltató jogosult megismerni, ugyanakkor biztosítani kell a levelezésben érintett harmadik személy azon jogát is, hogy az adatkezelés részleteiről tájékoztatást kapjon.

18.2. A Centrum által biztosított elektronikus levelező rendszer használata során, a személyes adatok védelme érdekében, az alábbi szabályokat kell betartani:

- a) a levelező rendszer hivatalos célra használható;
- b) a több mint száz e-mail címzett esetén a küldemény valamennyi címzettjét rejtett módon (titkos másolat mezőben) kell megadni a spam küldemények csökkentése érdekében;
- c) amennyiben a címzettek között a Centrum levelezőrendszerén kívüli címzett is szerepel, vizsgálni kell a b) pontban leírt módszer alkalmazásának szükségességét;
- d) a nagyobb mennyiségű személyes adatot tartalmazó küldemény továbbítása kizárólag technikai védelemmel (illetéktelen megnyitás ellen jelszóval védett Office dokumentumban, RMS védelemmel, jelszóval védett tömörített állományban stb.) engedélyezett;
- e) A személyes adatot tartalmazó elektronikus levelet a következő záradékkal kell ellátni:
„A jelen levélben kézbesített információ kizárólag a címzettnek szól, és bizalmas üzleti, illetve személyes adatokat tartalmazhat. Amennyiben nem Ön a levél címzettje, a levélben található információ felhasználása, vagy bármilyen módon történő közzététele, másolása vagy megosztása tilos. Amennyiben jelen levelet tévedésből kapta meg, kérem lépjen kapcsolatba a levél feladójával és az üzenetet haladéktalanul törölje a számítógépéről. A levél feladójának e-mail címe kifejezetten vállalati felhasználásra szolgál, a biztonsági szervezet – vezetői ellenőrzés céljából – betekinthez tartalmába, kérem erre a címre magánjellegű küldeményt, reklámanyagot ne küldjön!”.

18.3. A munkavállaló által használt e-mail postafiók ellenőrzése:

- a munkavállalót az ellenőrzést megelőzően tájékoztatni kell az ellenőrzés részleteiről,
- a munkáltató korlátozhatja az e-mail postafiók használatát,
- meghatározhatók azok a címek, ahonnan e-mail fogadható, illetőleg amelyekre küldhető,
- korlátozható a küldött/fogadott levél mellékletének terjedelme.

18.4. Amennyiben a felhasználó munkavégzésre irányuló jogviszonya megszűnik, a rendelkezésére bocsátott e-mail címet a munkaviszony megszűnésével egyidejűleg meg kell szüntetni. A levelezésre használt számítógép adattartalmára vonatkozóan a felhasználót nyilatkoztatni kell. A beérkező leveleket a feladónak automatikusan vissza kell küldeni, tájékoztatva őt arról, hogy az adott e-mail cím megszűnt, és megadni számára az adott feladatot a továbbiakban végző felhasználó elérhetőségét.

18.5. A kizárólag munkavégzés céljából biztosított e-mail postafiók esetén a munkáltatónak joga van a postafiókban lévő e-mailek fejlecének megtekintése után – ahol szerepel a küldő és a fogadó személye, e-mail címe, a levél megnevezése, a küldés időpontja, a levél mérete – a konkrét levél kiadását kérni a munkavállalótól. A munkavállaló a levél átadását csak a harmadik személy jogát sértő levéltitokra történő hivatkozással tagadhatja meg. Abban az esetben, ha az e-mail postafiókot kizárólag hivatalos használatra adták át számára és az abban található magánjellegű levelet a munkavállaló írta, vele szemben munkajogi szankciókat alkalmazhat a munkáltatói jogkörgyakorló.

18.6. Amennyiben egy munkavállaló tartós távolléte alatt, vagy munkaviszonyának megszűnését követően a személyhez rendelt e-mail postafiók ellenőrzése szükséges, vagy indokolt, az érintett munkavállaló által a levelező rendszerben a postafiókjához hozzáféréssel rendelkező másik munkavállaló – ha ilyen személy nincs, vagy nem tartózkodik a munkahelyen, akkor a munkáltató felkérésére a rendszer üzemeltetéséért felelős informatikus – jegyzőkönyv felvétele mellett betekinthez az e-mail postafiókba. Amelyik levélről egyértelműen megállapítható, hogy hivatalos tárgyú, átadható a munkáltatónak. A távollévő érintettet, az információs önrendelkezési jog maradéktalan érvényesülése érdekében tájékoztatni kell arról, hogy más személy az e-mail postafiókjá tartalmát megismerte.

19. VÉDENDŐ INFORMÁCIÓ KEZELÉSE

19.1. A munkavállaló köteles megőrizni a munkaköre betöltésével összefüggésben tudomására jutott védendő információt, amelynek közlése a munkáltatóra, vagy más személyre hátrányos következménnyel járhat.

20. A MUNKAHELYRE ÉRKEZŐ MAGÁNJELLEGŰ KÜLDEMÉNYEK KEZELÉSE

20.1. Magánjellegű levelezés folytatása a Centrumnál nem engedélyezett. Amennyiben ennek ellenére postai, vagy futár útján ilyen névre szóló küldemény érkezik, annak felbontása nem csak az érintett személyes adatai védelméhez, hanem a levéltitokhoz való jogának sérelmével is járhat, ezért azt más nem bonthatja fel, a címzettnek át kell adni, vagy a feladójának vissza kell küldeni.

20.2. Amennyiben kétség merül fel a levél hivatalos, vagy magánjellegét illetően, a címzett számára lehetőséget kell biztosítani a küldemény felbontására.

20.3. Ha egy levélről a felbontást követően derül ki, annak magánjellege, a borítékot vissza kell zárni és a téves felbontás tényéről készült jegyzőkönyvet mellékelve kell átadni az érintett munkavállalónak.

21. EGYÉB FELADATOK ÉS FELELŐSSÉG

Az érintett munkavállalókat felvételkor, illetve munkakörük megváltozása esetén, a munkakörük jellegéhez igazodóan, a kellő mértékig, dokumentált módon tájékoztatni szükséges az adatvédelem kérdéseiről, amelyért a munkáltatói jogkör gyakorlója a felelős.

22. AZ ADATVÉDELMI SZABÁLYOK MEGTARTÁSÁNAK ELLENŐRZÉSE

22.1. Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen szabályzat rendelkezései érvényesülésének ellenőrzésére jogosultak:

- a) a Centrum főigazgatója, kancellárja, főigazgató-helyettese, gazdasági vezetője.
- b) az adatvédelmi tanácsadó
- c) a jogszabályban erre felhatalmazott személy (például a NAIH tisztviselői)
- d) a Centrum által megbízott személy (pl. külső auditor).

22.2. Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

- a) adatkezelési szabályzat
- b) adatkezelési tájékoztató és adatvédelmi nyilatkozat
- c) az adatvédelmi nyilvántartásba történő bejelentés
- d) feliratok, piktogramok megléte
- e) a munkavállalók betekintési- és hozzáférési jogosultságának naprakészsége
- f) a fizikai biztonsági előírások érvényesülése
- g) a jelszavak időszakonkénti cseréje
- h) az adattovábbítási nyilvántartás vezetése
- i) adathordozók meglétének szűrőpróbaszerű ellenőrzése
- j) a selejtezés, megsemmisítés végrehajtására, dokumentálása
- k) a jelen szabályzat rendelkezéseinek betartása.

23. AZ ADATVÉDELMI RENDELKEZÉSEK MEGSÉRTÉSE ESETÉN KÖVETENDŐ ELJÁRÁS

23.1. Az adatvédelmi szabályok megsértése, vagy ennek közvetlen veszélye észlelése esetén, bárki közvetlenül az adatvédelmi kapcsolattartóhoz fordulhat. Az adatvédelmi kapcsolattartó a bejelentés megalapozottsága, illetve az adatvédelmi előírások megsértésének észlelése esetén annak megszüntetésére szólítja fel az adatkezelőt, és azokkal a munkavállalókkal szemben, akik a Centrum adatvédelmi és adatbiztonsági szabályzata előírásait megsértették, az érintett munkáltatói jogkörgyakorlójánál hátrányos jogkövetkezmény megállapítására vonatkozó munkáltatói intézkedést, esetlegesen tényfeltáró vizsgálatot kezdeményez. A megállapítás, illetve a tényfeltáró vizsgálat az adatvédelmi kapcsolattartó bevonásával történik.

23.2. A tényfeltáró vizsgálat lefolytatására, a vétkes kötelezettségszegés megállapítására, a hátrányos jogkövetkezmények és más munkajogi intézkedések alkalmazására a munkaviszonyra vonatkozó szabályok (Mt., belső szabályzatok, utasítások) irányadóak. A szankcióknak arányban kell állniuk a kötelezettségszegés súlyával és az okozott kárral.

24. ADATVÉDELMI INCIDENSEK KEZELÉSE

24.1. Az a munkavállaló, aki a Centrum által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan

hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést észlel, azt köteles a közvetlen vezetője útján haladéktalanul az adatvédelmi kapcsolattartónak bejelenteni, megadva a nevét, telefonszámát és/vagy e-mail címét, a szervezeti egységét, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e.

24.2. A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

24.3. A kapcsolattartó a bejelentést követően tájékoztatja az ügyvezetőt az adatvédelmi incidens bekövetkezéséről, megadva a bejelentő nevét, telefonszámát és/vagy e-mail címét, szervezeti egységét, továbbá a bejelentett adatvédelmi incidens tárgyát, azt, hogy az incidens informatikai rendszert érint-e, valamint a további, a bejelentő által tudomására hozott egyéb információkat.

24.4. Amennyiben a Centrum ellenőrzésre jogosult szervezeti egységei a feladataik ellátása során adatvédelmi incidenst észlelnek, a belső adatvédelmi felelőst értesítik.

24.5. A bejelentés megvizsgálása és az incidens kezelése

24.5.1. A belső adatvédelmi kapcsolattartó – informatikai rendszert érintő incidens esetén az érintett szervezeti egységgel együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 2 munkanapon belül teljesíteni.

24.5.2. Az adatszolgáltatásnak tartalmaznia kell

- I. az incidens bekövetkezésének időpontját és helyét,
- II. az incidens leírását, körülményeit, hatásait,
- III. az incidens során kompromittálódott adatok körét, számosságát,
- IV. a kompromittálódott adatokkal érintett személyek körét,
- V. az incidens elhárítása érdekében tett intézkedések leírását,
- VI. a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

24.5.3. Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens vizsgálatot igényel, annak végrehajtására az adatvédelmi kapcsolattartó felkéri az adatvédelmi szakértőt. A belső adatvédelmi kapcsolattartó szaktanácsadóként közreműködik a vizsgálat lefolytatásában.

24.5.4. A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az adatgazda egyetértésével dönt.

24.5.5. Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, kijelölt adatgazda esetében az adatgazda az adott intézkedések végrehajtását követő 2 munkanapon belül köteles az adatvédelmi kapcsolattartót tájékoztatni.

24.6. Az adatvédelmi incidens nyilvántartása

24.6.1. Az adatvédelmi incidensről az adatvédelmi kapcsolattartó nyilvántartást vezet.

A nyilvántartásba rögzíteni kell:

- a) az érintett személyes adatok körét,
- b) az adatvédelmi incidenssel érintettek körét és számát,
- c) az adatvédelmi incidens időpontját,
- d) az adatvédelmi incidens körülményeit, hatásait,
- e) az adatvédelmi incidens elhárítására megtett intézkedéseket,
- f) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

24.6.2. A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az adatvédelmi felelős megőrizni.

25. HATÁLYBA LÉPTETŐ RENDELKEZÉS

25.1. A szabályzat 2025. június 1. napján lép hatályba és visszavonásig érvényes. A szervezeti egységek vezetői gondoskodnak arról, hogy munkavállalóik a szabályzatban szabályozott – tevékenységükhöz kapcsolódó – ismereteket elsajátítsák.

25.2. A jelen szabályzatban foglalt előírásoknak történő megfelelés érdekében az adatkezelést végző szervezeti egységek vezetői gondoskodjanak az irányításuk alá tartozó adatkezelők felé az adatkezelések áttekintésére.