LECHNER
TUDÁSKÖZPONT

8../2022. számú ügyvezetői utasítás

A Lechner Tudásközpont Nonprofit Korlátolt Felelősségű Társaság Adatvédelmi Szabályzata

A Lechner Tudásközpont Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: Lechner Tudásközpont) fokozottan ügyel a személyes adatok védelmére, a kötelező jogi rendelkezések betartására, a biztonságos és tisztességes adatkezelésre. A Lechner Tudásközpont a jelen utasítás mellékletében szereplő szabályzatban foglaltak szerint a személyes adatokat bizalmasan kezeli, és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát megóvja és az adatvédelmi-, adatbiztonsági előírások érvényesülését garantálja.

Társaságunk fontosnak tartja minden természetes személy, legyen az foglalkoztatott, vagy ügyfél, vagy bármely más, harmadik személy adatkezeléshez és adatvédelemhez kapcsolódó jogának tiszteletben tartását és érvényre juttatását.

A Lechner Tudásközpont kötelezettséget vállal arra, hogy a rá bízott közfeladat ellátásával, illetve a tevékenyégével kapcsolatos adatkezelése megfelel a jelen utasítás mellékletében szereplő szabályzatban és a hatályos jogszabályokban meghatározott elvárásoknak.

Az utasításban foglaltak betartása a Lechner Tudásközpont minden munkavállalója számára kötelező. Jelen ügyvezetői utasítás a munka törvénykönyvéről szóló 2012. évi I. törvény 15. § (4) bekezdésére tekintettel a közzététel napján a munkavállalókkal közöltnek tekintendő.

A jelen ügyvezetői utasítás mellékletében szereplő szabályzat elkészítéséért, továbbá az annak legalább kétévente történő, valamint soron kívüli felülvizsgálatáért a Cégjogi Főosztály – az adatvédelmi tisztviselő bevonásával –a felelős.

A jelen ügyvezetői utasítás mellékletében szereplő szabályzat aktuális változatát a hatályba lépés napján elektronikus formában közzé kell tenni a Lechner Tudásközpont belső utasítás- és szabályzatnyilvántartásában.

Az ügyfelek és külső harmadik személyek számára az adatvédelemről szóló és rájuk vonatkozó adatkezelési tájékoztatókat a Lechner Tudásközpont honlapján (www. lechnerkozpont.hu) közzé kell tenni.

Jelen Szabályzat a kihirdetés napján lép hatályba.

Budapest, 2022. 02. 11. ....

LECHNER NONPROFIT KFT.
1111 BUDAPEST, BUDAFOKI ÚT 59.
ADÓSZÁM: 24252218-2-43

.....
Kolossa József
ügyvezető

LECHNER TUDÁSKÖZPONT

Készítette a Cégjogi Főosztály az adatvédelmi tisztviselő bevonásával:

dr. Stefán Kornélia és dr. Botos Norbert

2022. 02. 11. .....

Véleményezte a Stratégiai és Operatív Igazgatóság nevében:
2022. 02. 11.
.....

Véleményezte a Nyilvántartás-fejlesztési és –üzemeltetési Igazgatóság nevében:
2022. .02. 11.
.....

Véleményezte az Ingatlan-nyilvántartási és Geodéziai Igazgatóság nevében:
2022. 02. 11.
.....

Véleményezte az Üzemi Tanács nevében:
2022. 02. 11.
.....

Ellenőrizte a Jogi Igazgatóság vezetője: dr. Bajzát Edina
2022. 02. 11.
.....

LECHNER
TUDÁSKÖZPONT

A Lechner Tudásközpont Nonprofit Korlátolt Felelősségű Társaság Adatvédelmi Szabályzata

Lechner Nonprofit Kft.

LECHNER TUDÁSKÖZPONT

1 Tartalom

Bevezetés

1. A Lechner Tudásközpont Nonprofit Korlátolt Felelősségű Társaság (a továbbiakban: Lechner Tudásközpont, Társaság vagy Adatkezelő) jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit.
2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során a Lechner Tudásközpont kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR, vagy Általános Adatvédelmi Rendelet), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alkalmazandó rendelkezései, valamint a Társaságra irányadó egyéb jogszabályok előírásai szerint kezelni.
3. A Lechner Tudásközpont a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a) a jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
   b) a célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat a Társaság nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
   c) az adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
   d) a pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
   e) a korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
   f) az integritás és bizalmas jelleg elve: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;
   g) a beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve az Általános Adatvédelmi Rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;
   h) az alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából

szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül arra illetéktelen személyek számára ne válhassanak hozzáférhetővé.

4. A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre vonatkozó speciális szabályzatokban foglalt rendelkezések mellett a jelen Szabályzat előírásai szerint eljárni azzal, hogy amennyiben a speciális szabályzat a jelen Szabályzattal ellentétes rendelkezést tartalmaz, akkor jelen Szabályzat alkalmazandó.
5. Valamennyi foglalkoztatott kötelezettsége annak bejelentése, ha a Szabályzat megkerüléséről vagy megsértéséről szerez tudomást, vagy ennek gyanúja merül fel. Bejelentés elsődlegesen a szokásos bejelentési csatornákon teendő, vagyis a közvetlen felettes, a szervezeti egység szerinti felsővezető, vagy az adatvédelmi tisztviselőnek a megkeresésével.

1 Általános rendelkezések

1.1 A Szabályzat célja

6. A Szabályzat célja, hogy meghatározza a Lechner Tudásközpontnál zajló adatkezelések jogszerű kereteit, biztosítsa az adatvédelem Alaptörvényben foglalt elveinek és az információs önrendelkezési jognak az érvényesülését, elősegítse az adatbiztonság követelményeinek való megfelelést, megakadályozza a jogosulatlan adatkezelést.
7. E Szabályzat célja továbbá, hogy a vonatkozó jogszabályi rendelkezések keretei között meghatározza az Adatkezelőnél vezetett személyes adatokat tartalmazó nyilvántartások szabályos rendjét, valamint biztosítsa az adatvédelem alapjogi elveinek, az információs önrendelkezési jognak és az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok jogosulatlan megváltoztatását és nyilvánosságra hozatalát.
8. A Szabályzat a Lechner Tudásközpont által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.

2 A Szabályzat hatálya

2.1 A Szabályzat személyi hatálya

9. E Szabályzat személyi hatálya kiterjed a Lechner Tudásközponttal munkaviszonyban, megbízási vagy más munkavégzésre irányuló egyéb jogviszonyban álló személyekre. E Szabályzat személyi hatálya kiterjed továbbá a Lechner Tudásközponttal az előzőekben felsorolt jogviszonyban nem álló, de a Társaság tevékenység-ellátásával összefüggő, valamint a vele szerződéses vagy egyéb kapcsolatban álló személyesadat-kezelést végző személyekre, gazdasági társaságokra és a Társaság ügyfeleire.
10. A Lechner Tudásközpont megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra a Lechner Tudásközpont által kötött szerződésben a GDPR 28. cikkének (*„Az adatfeldolgozó”*) megfelelően rendelkezni kell arról, hogy a Lechner Tudásközpont által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

11. A Szabályzat hatálya a jogi személyek, illetve a jogi személyeknek nem minősülő szervezetek adataival kapcsolatos adatkezelésre, adatfeldolgozásra nem terjed ki.

2.2 A Szabályzat tárgyi hatálya

12. A Szabályzat tárgyi hatálya kiterjed a Lechner Tudásközpont, mint Adatkezelő által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül. Jelen Szabályzat hatálya eszerint kiterjed a Lechner Tudásközpont egyes szervezeti egységei közötti, valamint a Lechner Tudásközpont, mint Adatkezelő által igénybe vett adatfeldolgozók felé irányuló adatáramlásra, valamint az Adatkezelő és más Adatkezelőkkel való személyes adatokat érintő kommunikációra. Kiterjed továbbá az Adatkezelő székhelyén folyó – természetes személyeket érintő – valamennyi adatkezelésre, adattovábbításra, információ átadásra, az ezen adatkezelés, információátadás tárgyát képező adat jelen Szabályzatban meghatározottak szerinti kezelésével és védelmével kapcsolatos tevékenységekre.
13. A jelen Szabályzat tárgyi hatálya nem terjed ki a Lechner Tudásközpont által kezelt, jogszabály alapján közérdekű vagy közérdekből nyilvános adatra, melyek kezelésére a Közérdekű Adatok Megismerésére Irányuló Igények Teljesítésének Rendjéről szóló Szabályzatban foglaltak az irányadók.
14. A jelen Szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az informatikai biztonsági keretszabályzatról szóló 2/2017. számú utasítás rendelkezik a Társaságnál.

3 Alapfogalmak

15. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3-4., 6., 11-13., 16-17., valamint a 21. és 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:
    a) adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik;
    b) Adatkezelési Tevékenységek Nyilvántartása: jelen utasítás 14. fejezetében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;
    c) adatkezelésért felelős szervezeti egység: a Lechner Tudásközpont azon igazgatósága(i), amely(ek)nek feladatkörébe tartozik a Társaság kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése;
    d) adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság);
    e) adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatkezelési koordinátor) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes

adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja;

f) adatvédelmi incidens típusai (jellege): személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.;

g) adatkezelési koordinátor: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen Szabályzatban, illetve az adatkezelésről szóló más belső szabályozó dokumentumokban meghatározottak szerint az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről;

h) adatvédelmi tisztviselő: a Lechner Tudásközpont szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat a Társaság jelen Szabályzatában foglaltak szerint ellátó, a Lechner Tudásközponttal foglalkoztatási vagy megbízási jogviszonyban álló természetes személy;

i) álnevesítés (pszeudonimizálás): 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;

j) deperszonalizálás (anonimizálás): a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását;

k) érdekmérlegelési teszt: jogos érdeken [GDPR 6. cikk (1) bekezdés f) pont] alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adataik védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását;

l) informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve a Lechner Tudásközpont információbiztonsági vezetőjét is;

m) titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül;

n) törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható deperszonalizálással (anonimizálással) [j) pont] is;

o) ügyvitel: a Lechner Tudásközpont tevékenységére vonatkozó jogszabályokban a Társaság részére meghatározott közfeladatok ellátásával összefüggő eljárás.

4 A Szabályzathoz kapcsolódó jogszabályok és belső szabályzatok

A Szabályzat alkalmazása során különösen az alábbi jogszabályok és belső szabályzatok előírásait kell figyelembe venni:

	Magyarország Alaptörvénye
GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lásd: Infotv. 2. § (2) és (4) bekezdése]
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
Ptk.	2015. évi V. törvény a Polgári Törvénykönyvről
E-ügyint. tv.	2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
7/2021. számú utasítás	a Lechner Tudásközpont Szervezeti és Működési Szabályzata
2/2017. számú utasítás	a Lechner Tudásközpont Informatikai Biztonsági Keretszabályzata és Információvédelmi Szabályzata
23/2020. számú utasítás	a Lechner Tudásközpont Archiválási Szabályzata
8/2021. számú utasítás	a Lechner Tudásközpont Iratkezelési Szabályzata
13/2021. számú utasítás	a Lechner Tudásközpont Szabályzatkezelési Rendje

5 Az adatvédelmi tevékenység szervezete és irányítása

5.1 Az adatvédelmi tevékenység ellátásában résztvevők

16. A Lechner Tudásközpont tevékenységi körébe tartozó feladatok ellátása során a személyes adatok adatkezelője a Társaság, amely az adatkezelési tevékenységet az erre felhatalmazott szervezeti egységei (a továbbiakban: adatkezelő szervezeti egység) útján végzi.
17. Az adatvédelmi tevékenység irányításában és ellátásában a Lechner Tudásközpont szervezeti egységei a Társaság Szervezeti és Működési Szabályzatában meghatározott feladatkörükön belül a jelen Szabályzatban foglaltak szerint vesznek részt.
18. Az ügyvezető felelős azért, hogy a Lechnert Tudásközpont – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:
    a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;

b) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
c) felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
d) gondoskodik az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
e) kinevezi a Lechner Tudásközpont adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
f) biztosítja a Lechner Tudásközpont adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket.

19. A Lechner Tudásközpont szervezeti egységeinek vezetői az irányításuk alá tartozó szervezeti egység tekintetében:
a) betartják és betartatják az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírásokat; az adatvédelmi tisztviselővel, a Jogi Igazgatósággal, továbbá az informatikai szakterülettel együttműködve gondoskodnak az adat- és titokvédelmi, valamint a biztonsági és információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról;
b) kijelölik az irányításuk alá tartozó szervezeti egység adatkezelési koordinátorát (22. pont);
c) gondoskodnak arról, hogy az irányításuk alá tartozó szervezeti egységek felelősségi körébe tartozó nyilvántartások naprakészek, megbízhatóak legyenek;
d) gondoskodnak arról, hogy az irányításuk alatt álló személyek az adatkezelés meghatározott feltételeinek megfelelően járjanak el [GDPR 32. cikk (4) bek.];
e) az adatkezelési koordinátor 6. fejezet szerinti előterjesztésére – a Lechner Tudásközpont döntés előkészítésre vonatkozó szabályainak megfelelően – döntenek a jelen Szabályzatban, illetve az adatkezeléssel járó folyamatot szabályozó egyéb belső szabályzatokban a feladat- és hatáskörébe utalt kérdésekben.

20. Az informatikai szakterület a Lechner Tudásközpont Szervezeti és Működési Szabályzatában, valamint a Társaság Informatikai Biztonsági Szabályzatában meghatározott feladatkörében:
a) ellátja az informatikai biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen a Társaság Informatikai Biztonsági Szabályzatában meghatározott feladatokat;
b) ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításával, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat;
c) az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja a Társaság Informatikai Biztonsági Szabályzatában meghatározott, hatáskörébe tartozó információbiztonsági feladatokat, valamint a rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidens-felderítési- és kezelési tevékenység támogatását;
d) az érintett szervezeti egységek vezetőivel együttműködve gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

21. A Jogi Igazgatóság
    a) a szervezeti egység adatkezelési koordinátorától kapott információk alapján közreműködik a szervezeti egységgel kapcsolatos, az adatkezelőt terhelő döntések előkészítésében és az intézkedések végrehajtásában (pl. érdekmérlegelési teszt elvégzése, adatvédelmi hatásvizsgálat lefolytatása);
    b) a Lechner Tudásközpont szervezeti és működési rendje szerint biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék a Társaság adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során;
    c) biztosítja a Lechner Tudásközpont képviseletét az érintett által a Társaság ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve a Társaság által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.
22. Igazgatóságonként legalább egy személy adatkezelési koordinátort kell kijelölni.
23. Adatkezelési koordinátornak olyan személyt kell kijelölni, aki az adott szervezeti egység tevékenységét, az ahhoz kapcsolódó adminisztratív folyamato(ka)t átlátja, illetve a szervezeti egység tevékenységét támogató informatikai rendszerekről kellő ismeretekkel bír. Egy adatkezelési koordinátor hatáskörébe több szervezeti egység is tartozhat, illetve egy szervezeti egységnek több adatkezelési koordinátora is lehet. Az adatkezelési koordinátori kijelölést, hatáskört és a feladatokat írásba kell foglalni (pl. a munkaköri leírásban vagy a megbízásról szóló dokumentumban szerepeltetni kell).
24. Az adatkezelési koordinátor a felelősségi körébe tartozó szervezeti egység(ek) feladatkörén belül jelen Szabályzat és egyéb, a szervezeti egység tevékenységét érintő belső szabályozás szerint:
    a) figyelemmel kíséri az adott szervezeti egység tevékenységét adatkezelési szempontból, az adatkezeléssel kapcsolatos bárminemű változás vagy arra utaló szándék (pl. tervezett új adatkezelés, illetve adatkezelés megszüntetése vagy módosítása) egyeztetést kezdeményez az adatvédelmi tisztviselővel;
    b) figyelemmel kíséri, hogy az adott szervezeti egység a személyes adatokat az adatkezelésre vonatkozó belső szabályozásnak megfelelően kezeli-e, az esetleges eltéréseket jelzi az adatvédelmi tisztviselőnek és az adott szervezeti egység vezetőjének egyidejű értesítése mellett;
    c) közreműködik, az Adatkezelési Tevékenységek Nyilvántartásának naprakészen tartásában, az esetleges változásokat jelzi az adatvédelmi tisztviselőnek;
    d) adatvédelmi incidens gyanúja esetén az eseményt bejelenti az erre vonatkozó eljárásrend szerint vagy kétség esetén egyeztet az adatvédelmi tisztviselővel;
    e) segíti a Jogi Igazgatóság feladatainak ellátását azzal, hogy információt szolgáltat a szervezeti egység tevékenységéről, és közreműködik a szervezeti egységgel kapcsolatos, az adatkezelőt terhelő döntések előkészítésében és az intézkedések végrehajtásában (pl. érdekmérlegelési teszt elvégzése, adatvédelmi hatásvizsgálat lefolytatása);
    f) közreműködik az adatvédelmi tisztviselőnek az adott szervezeti egységet érintő adatkezelési gyakorlatra vonatkozó vizsgálataiban.

5.2 Az adatvédelmi tisztviselő

25. A Lechner Tudásközpont ügyvezetője adatvédelmi tisztviselőt nevez ki az olyan, a Társasággal foglalkoztatási jogviszonyban álló természetes személyek közül, aki megfelel az erre a

tisztségre vonatkozó, a Társaság Szervezeti és Működési Szabályzatában előírt követelményeknek.

26. Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül az ügyvezető döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget az adatvédelmi tisztviselői feladatokkal. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a jogi igazgató útján a Lechner Tudásközpont ügyvezetőjének tartozik felelősséggel.
27. Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott minden olyan információ tekintetében, amely nem minősül közérdekű vagy közérdekből nyilvános adatnak.
28. Az adatvédelmi tisztviselő nevét és elérhetőségeit a Lechner Tudásközpont honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. A Lechner Tudásközpont továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Hatósággal.
29. Az adatvédelmi tisztviselő véleményét – a szervezeti és működési rend, valamint jelen Szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.
30. A Lechner Tudásközpont elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében a Társaság biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásához szükséges időt és forrást. A Lechner Tudásközpontnál nem lehet adatvédelmi tisztviselő az a természetes személy, aki a Társaság adatkezelési tevékenysége céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen az ügyvezető és az adatkezelésért felelős szervezeti egység vezetője, valamint a helyetteseik, az együttes vagy önálló cégjegyzésre vagy bankszámla feletti rendelkezésre jogosult vagy a Társaság működése szempontjából meghatározó jelentőségű munkavállaló, továbbá a belső ellenőr, illetve az információbiztonsági vezető.
31. <u>Az adatvédelmi tisztviselő a következő feladatokat látja el:</u>
    a) tájékoztat és szakmai tanácsot ad a Társaság vagy az adatfeldolgozó, továbbá az adatkezelést végző foglalkoztatottak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
    b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Társaság vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
    c) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
    d) vezeti az Adatkezelési Tevékenységek Nyilvántartását;
    e) kivizsgálja – az érintett szakterületek bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

f) a Jogi Igazgatóság Cégjogi Főosztályával és az informatikai szakterülettel együttműködve elkészíti az adatvédelmi szabályzatot;
g) a Képzési és Oktatási Osztállyal együttműködve gondoskodik az adatvédelmi ismeretek oktatásáról;
h) a Jogi Igazgatósággal együttműködve tájékoztatást nyújt, tanácsot ad a személyes adatok kezelésére vonatkozó előírásokról;
i) személyes adatot is kezelő (új) informatikai rendszer fejlesztése során közreműködik a beépített adatvédelem alapelve érvényesülésének érdekében, vagy ha szükséges, az adatvédelmi hatásvizsgálat lefolytatásában;
j) a Lechner Tudásközpont adatvédelmi helyzetéről éves összefoglaló jelentést készít az ügyvezetőnek;
i) együttműködik a Hatósággal;
j) az adatvédelmi incidensek kezelésével kapcsolatban ellátja a jelen Szabályzat szerinti feladatokat, adatvédelmi incidens esetén bejelentéssel él a Hatóság irányába, és az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

32. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.
33. Az adatvédelmi tisztviselők konferenciáján a Lechner Tudásközpontot az adatvédelmi tisztviselő képviseli, aki az adatvédelmi tisztviselők konferenciáján elhangzottakról írásban tájékoztatja a Társaság ügyvezetőjét és a szervezeti egységek vezetőit.

6 Adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

6.1 Adatkezelés bevezetésével kapcsolatos feladatok

34. Jogszabályban elrendelt, vagy jogszabály rendelkezése miatt szükséges, vagy a Lechner Tudásközpont döntése alapján létrehozandó személyes adatok kezelésével járó új nyilvántartás vagy nyilvántartási rendszer (a továbbiakban együtt: adatkezelés) bevezetése esetén, továbbá ha a meglévő adatkezelésben kezelt személyes adatok új célú felhasználását vagy még nem kezelt személyesadat-kategóriák felvételét, tárolását, harmadik személynek továbbítását tervezik (a továbbiakban együtt: új adatkezelés), az új adatkezelés bevezetése során a döntés előkészítés rendjére vonatkozó belső szabályokat e fejezet rendelkezéseit figyelembe véve kell alkalmazni.
    a) Az új adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban a Jogi Igazgatóság az adatvédelmi tisztviselő felügyelete mellett, a leendő adatkezelésért annak tárgya szerint felelős szakterület/szervezeti egység(ek) adatkezelési koordinátorával együttműködve:
        aa/ meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és erről írásbeli javaslatot készít a döntésre jogosultnak [GDPR 4. cikk 7. és 16. pont];
        ab/ szükség esetén tájékoztatja a döntésre jogosultat arról, hogy egy meglévő adatkezelés eltérő, új célja összeegyeztethető-e az adatkezelés eredeti céljával, és így hatással van-e a tervezett adatkezelés jogalapjára [GDPR 6. cikk (4) bek.];

ac/ amennyiben az új adatkezelés jogalapja a jogos érdek lehet [GDPR 6. cikk (1) bek. f) pont], elkészíti az érdekmérlegelési teszt tervezetét;

ad/ dokumentálja az adatvédelmi hatásvizsgálat el nem végzésének indokait, vagy elvégzi az adatvédelmi hatásvizsgálatot [42-53. pont];

ae/ szükség esetén javaslatot tesz automatizált döntéshozatali módszer, illetve profilalkotási módszer alkalmazására [GDPR 22. cikk (1) bek.];

af/ szükség esetén megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], továbbá ha közös adatkezelés vagy adatfeldolgozó bevonása miatt szükséges, a megfelelő szerződéses rendelkezéseket;

ag/ megfogalmazza az új adatkezelésre, vagy a meglévő adatkezelés módosítására, illetve az a profilalkotási és automatizált döntéshozatali módszerekre vonatkozó információkkal kiegészíti az adatkezelési tájékoztatót [GDPR 13-14. cikk];

ah/ az informatikai szakterület közreműködésével gondoskodik az új adatkezelésről szóló új vagy módosított tájékoztatás könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];

ai/ az Adatkezelési Tevékenységek Nyilvántartásában rögzíti az új adatkezelés adatait, illetve átvezeti a már nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.];

aj/ megvizsgálja – amennyiben ennek szükségessége felmerül –, hogy személyes adatok harmadik országba továbbíthatók-e [GDPR 49. cikk (1) bek.];

b) az informatikai szakterület a személyes adatot kezelő rendszer fejlesztése és beszerzése során közreműködik:

ba/ a célhoz kötött adatkezelés és az adattakarékosság elvének megfelelően gyűjtött adatokra vonatkozóan a beépített és alapértelmezett adatvédelem elveinek érvényesüléséről;

bb/ annak biztosításában, hogy az adathordozhatóság, adattörlés és adattisztítás célú módosítások szabályozott és dokumentált módon valósuljanak meg;

bc/ annak biztosításában, hogy az adatvédelmi tájékoztatók és nyilatkozatok könnyen elérhetők legyenek bárki számára;

bd/ annak biztosításában, hogy az adatkezeléssel kapcsolatos ügyfélrendelkezéseket (pl. hozzájáruló nyilatkozatokat vagy azok visszavonását) visszakereshető formában tárolják;

be/ az adatok sértetlenségével, bizalmasságuk megőrzésével és az üzletmenet-folytonossággal kapcsolatos kontrollok (pl. változáskezelés, magas rendelkezésre állás, jogosultságkezelés, adatrejtő eljárások, incidenskezelés támogatása) tervezéskori érvényesítésében, illetve dokumentált meglétében;

bf/ az adott adatkezelés egyedi adatbiztonsági intézkedéseinek meghatározásában.

35. Az adatkezelés során (informatikai rendszerben kezelt személyes adatok esetén az informatikai rendszer üzemeltetési szakaszában) az informatikai biztonsági követelmények betartása az Informatikai biztonságra vonatkozó belső szabályozás szerint történik.

36. Amennyiben az adatkezelési tevékenység során szükségessé válik az érintett személyazonosságának vagy bármely más, rá vonatkozó tény (pl. iskolai végzettség) okmánnyal/okirattal való igazolása, akkor az igazolásként bemutatott okmányról és/vagy okiratról kizárólag abban az esetben lehet fénymásolatot készíteni, ha ezt jogszabály kifejezetten elrendeli. Erről szóló jogszabályi rendelkezés hiányában az érintett

személyazonosságának vagy bármely más, rá vonatkozó tény igazolása céljából történt okmány- vagy okirat bemutatásról és a Társaság foglalkoztatottja által történt megtekintésről feljegyzést kell készíteni, és a vonatkozó ügyiratban kell elhelyezni.

6.2 Adatkezelés megszüntetésével kapcsolatos feladatok

37. Amennyiben a Társaságnál egy (személyes adatra vonatkozó) adatkezelési tevékenység megszűnik, az adatvédelmi tisztviselő felügyelete alatt a Jogi Igazgatóság az Adatkezelési Tevékenységek Nyilvántartásában az adatkezelést archív státuszba kell tenni és a kapcsolódó adatkezelési tájékoztatót is archiválni kell.

6.3 Az érdekmérlegelési teszt elvégzésének módszertana

38. Amennyiben a Társaság valamely adatkezelésének a Társaság vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bek. f) pont], érdekmérlegelési tesztet kell dokumentáltan elvégezni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.
39. Az érdekmérlegelési tesztet a Jogi Igazgatóság megbízottja végzi el az adatvédelmi tisztviselő bevonásával. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.
40. Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések (41. pont) köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába, és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani a mérlegelés során.
41. Az érdekmérlegelési teszt részei:
    a) a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok (körének vagy típusának) meghatározása;
    b) az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?);
    c) az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?);
    d) az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése;
    e) a személyes adatok védelme biztosítékainak leírása;
    f) az érdekmérlegelési teszt eredménye.

6.4 Az adatvédelmi hatásvizsgálat elvégzésének módszertana

42. Ha az adatkezelés valamely, különösen az új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve, az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokkal járnak, egyetlen adatvédelmi hatásvizsgálat (a továbbiakban: hatásvizsgálat) keretei között is értékelhetők.
43. A hatásvizsgálat elvégzésének szükségességéről az adatvédelmi tisztviselő dönt.
44. A hatásvizsgálatot a Jogi Igazgatóság végzi el az adatvédelmi tisztviselő bevonásával. A hatásvizsgálat megállapításait írásban kell rögzíteni. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

45. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben [https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf] szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.
46. A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet (jogait) jelentős mértékben érinti.
47. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver található a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján [https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html].
48. A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:
    a) az adatkezelésért felelős szervezeti egységet és a tervezett közös adatkezelő vagy adatfeldolgozó megjelölését;
    b) az adatkezelés célját és jogalapját, az adatkezeléstől várt előnyöket, az adatkezelés szükségességét, az adatkezelés terjedelmét (időben és a kezelt adatok volumenében);
    c) az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
    d) azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást (ideértve az adatfeldolgozás céljából történő adatküldést is);
    e) az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
    f) az adatkezelés folyamatának a leírását.
49. A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni:
    a) az adatkezelés szükségességének és arányosságának biztosítékait, és
    b) az érintett jogait biztosító garanciák érvényesülését.
50. A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.
51. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
    a) a 48-50. pontban meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
    b) a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
    c) annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.
52. A hatásvizsgálat megállapításait az adatkezelési tevékenységbe vissza kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.
53. A hatásvizsgálatot legalább évente, dokumentáltan felül kell vizsgálni, szükség esetén újra el kell végezni.

7 Az érintetti jogok gyakorlásának elősegítése

7.1 Az adatkezelési tevékenység nyilvánossága

54. A Lechner Tudásközpont a honlapján közzéteszi:
    a) a Társaság Általános Adatkezelési Tájékoztatóját;
    b) a Társaság egyes adatkezelési tevékenységeihez kapcsolódó Különös Adatkezelési Tájékoztatókat (a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatók kivételével);
    c) közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;
    d) tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az Adatkezelő és az adatvédelmi tisztviselő elérhetősége, a Hatóság elérhetősége).
55. A Lechner Tudásközpont szervezeti egységeinek vezetői gondoskodnak arról, hogy az adatvédelemmel kapcsolatos szabályzatok és tájékoztatók a Társaság belső tájékoztatási fórumán rendelkezésre álljanak.
56. Az adatkezelés megkezdéskor az érintettek számára biztosítani kell a GDPR 13. cikk szerinti tájékoztatást és lehetőség szerint gondoskodni kell annak bizonyíthatóságáról. Példák: új dolgozó belépésekor az általános és a különös adatkezelési tájékoztatók tudomásulvételéről szóló nyilatkozat egy – az érintett által aláírt – példányát a foglalkoztatott személyi anyagába le kell fűzni, internetes regisztráció esetén egy jelölőnégyzetet bejelölésével nyilatkozik az érintett a tájékoztatás tudomásul vételéről.
57. A Lechner Tudásközpont kezelésében lévő közérdekű adatok és közérdekből nyilvános adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik.

7.2 Korlátozottan cselekvőképes személyek tájékoztatáshoz való jogának biztosítása

58. A Társaság szervezeti egységeinek vezetői az adatkezelési koordinátorok közreműködésével gondoskodnak arról, hogy a Lechner Tudásközponttal kapcsolatba kerülő, korlátozottan cselekvőképes személyek törvényes képviselői, illetve – állapotuktól függően – a korlátozottan cselekvőképes személyek is megfelelő tájékoztatást kapjanak a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy az adatkezelésre vonatkozó tájékoztatást közli a gondnoksága alatt álló érintettel.

7.3 Korlátozottan cselekvőképes személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

59. A Lechner Tudásközpont szervezeti egységeinek vezetői az adatkezelési koordinátorok közreműködésével gondoskodnak arról, hogy a Társasággal kapcsolatba kerülő korlátozottan cselekvőképes személyek tekintetében – amennyiben az adatkezelés az érintett hozzájárulásán alapul – a személyes adatok kezeléséhez való hozzájárulást törvényes képviselőjük adja meg.
60. A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.
61. Amennyiben az érintett törvényes képviselői (pl.: szülői felügyelet gyakorlására jogosult szülők) eltérő nyilatkozatot tesznek az adatkezeléshez való hozzájárulásról, úgy az adatkezeléshez való hozzájárulást meg nem adottnak kell tekinteni.

8 Az érintettől származó kérelmek, panaszok megválaszolásának rendje

62. Az egyes belső szabályzatoknak az érintettek adatainak felvételére, módosítására vagy helyesbítésére, illetve törlésére vonatkozó rendelkezései alkalmazását jelen Szabályzat nem érinti, az adatvédelmi tisztviselő azonban bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá a Hatóság vagy bíróság döntése végrehajtásaként – az említett szabályzatokban meghatározott hatásköri és eljárási rendtől függetlenül kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (az adatok zárolását).
63. A Lechner Tudásközponthoz érkező beadványokat esetről esetre és a beadvány tárgyával összefüggő adatkezelési tevékenység figyelembevételével kell megítélni, továbbá a Társaság Panaszkezelési Szabályzatában foglaltaknak megfelelően kell – a GDPR 12. cikkében írt határidők figyelembevételével – elintézni, az alábbi kiegészítésekkel és eltérésekkel:
    a) a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell;
    b) az érintetti panaszok kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során az érintett szervezeti egységek kötelesek az adatvédelmi tisztviselővel együttműködni. A személyes adatok kezelését, illetve a GDPR szerinti jogok gyakorlását érintő panasz megalapozottsága esetén az adatvédelmi tisztviselő az adatkezelésért felelős szervezeti egység(ek)nél intézkedést kezdeményez a panasz kiváltó okainak orvoslására, az érintett folyamatok felülvizsgálatára, valamint – szükség esetén – a személyi felelősség megállapítására;
    c) bármely beadvány esetén, a beadvány intézésért felelős szervezeti egység kérheti az adatvédelmi tisztviselő véleményét a tekintetben, hogy a beadvány adatvédelmi vonatkozású – e;
    d) az érintettnek saját adatai kezeléséről akár szóbeli (pl. telefonon történő), akár személyes megjelenés nélküli (pl. elektronikus levélben kért) tájékoztatás csak egyértelmű személyazonosítás után adható. Amennyiben a tájékoztatást kérő (beadványozó) nem azonosítható, vagy kétség merül fel a beadványozó személyazonosságát illetően, az egyértelműen elutasítandó beadvány kivételével meg kell kísérelni a beadványozó személyének azonosítását, beleértve a személyes megjelenés ajánlását. Ilyen esetekben a GDPR 12. cikk (3) bekezdése szerinti határidő a beadványozó sikeres azonosításakor kezdődik;
    e) amennyiben a beadványt előreláthatóan nem lehet a GDPR 12. cikk (3) bekezdése szerinti határidőben megválaszolni, a beadványozót a lehető a legrövidebb időn belül, legkésőbb 30. napon elküldött levélben vagy elektronikus üzenetben tájékoztatni kell a határidő meghosszabbításának szükségességéről, okairól és az új határidőről;
    f) amennyiben a beadványt a beadványozó kérelme ellenére nem lehet, vagy nem célszerű elektronikus úton megválaszolni (a kért dokumentumokat nem lehet vagy nem célszerű ilyen úton elküldeni, például video felvétel esetén), fel kell venni a kapcsolatot a beadványozóval annak érdekében, hogy kölcsönösen elfogadható megoldást találjanak. Különösen indokolt a beadványozóval a kapcsolatfelvétel, ha a beadványozó különleges adat megküldését kéri nem biztonságos elektronikus úton. A kapcsolatfelvételre olyan időben kell sort keríteni, hogy a beadványt akkor is meg lehessen válaszolni a határidő betartásával, ha a beadványozó ragaszkodik a nem biztonságos elektronikus úthoz vagy még nincs Ügyfélkapu regisztrációja;

g) elektronikus levél (e-mail) útján személyes adat úgy küldhető, ha az adatok bizalmassága, integritása és rendelkezésre állása biztosítható (pl. jelszavas védelemmel ellátott titkosított állomány vagy hivatkozás küldése egy jelszóval védett tárhelyre és a jelszót külön csatornán küldik el;

h) kivételes esetben, az érintett kifejezett kérésére vagy beleegyezésével és csak oly módon küldhető e-mailben személyes adat, ha előzőleg az érintett figyelmét felhívták a kockázatokra, és az érintett ezek után megerősíti a szándékát, egyúttal tudomásul véve az Társaság felelősségkizáró nyilatkozatát.

64. Amennyiben az adott adatkezelési tevékenységről szóló belső szabályozás – figyelemmel az adatkezelés tárgyára – másként nem rendelkezik, a személyazonosítás:

a) személyes megjelenés során a személyazonosságot igazoló okmány (pl. személyazonosító igazolvány, útlevél) bemutatásával,

b) személyes megjelenés hiányában pedig a természetes személyazonosító adatok (név, születési hely és idő, anyja neve), valamint legalább egy olyan adat (pl. ügyfél azonosító) megadásával történik, amelyet mind az érintett, mind a Társaság ismer, illetéktelen személy számára azonban nem hozzáférhető.

65. A személyazonosítás során a Lechner Tudásközpont személyazonosítást végző alkalmazottja köteles meggyőződni arról, hogy az érintett által bemutatott okmány adatai, vagy az érintett 64. b) alpont szerinti adatai azonosak-e a Társaság nyilvántartásában szereplő adatokkal. Amennyiben a személyazonosítás nem egyértelmű (az érintett által bemutatott okmány vagy a személyes megjelenés nélkül megadott adatai és a Társaság által nyilvántartott adatok között eltérés van), a beadvány elintézése mindaddig nem folytatható, amíg az érintett hitelt érdemlően nem igazolta magát.

66. Az adatvédelmi beadványokról olyan ügyirat-nyilvántartást szükséges vezetni, amely segítségével bármikor egyértelműen azonosíthatóak a GDPR által előírt érintetti jogokkal kapcsolatos beadványok, továbbá nyomon követhetők a beadványok elintézése során tett intézkedések, valamint a rendelkezésre álló adatokból bármikor statisztika készíthető a következő szempontok szerint:

a) adott időszakban érkezett beadványok száma, típus szerinti bontásban is;

b) a beadványok beérkezésének módja;

c) a beadványok megválaszolásának átlagos időtartama;

d) az elutasított beadványok száma, és azok okai;

e) a válaszadás módja.

9 Más szervtől érkező megkeresés teljesítése, adattovábbítás

67. A Lechner Tudásközpont adatkezelőként dönt a más szervtől (minisztérium, nyomozó hatóság stb.) érkező, személyes adat vagy személyes adatot tartalmazó tárgy (pl. biztonsági kamera felvétele) szolgáltatását kérő megkeresések (a továbbiakban együtt: megkeresés) teljesítéséről. A megkeresés teljesítése előtt esetről esetre mérlegelni kell, hogy az adatkérés teljesítése kötelező (jogszabály írja elő) vagy mérlegelhető (jogos érdeken alapul), továbbá, hogy a megkeresés és a teljesítése megfelel-e a jogszabályi feltételeknek (az arra jogosult küldte-e a megkeresést, a Társaságnak van-e jogalapja az adattovábbításhoz, a megkeresésben szereplő információk teljesek-e és elegendőek-e a megkeresés teljesítéséhez stb.).

68. A megkeresésre adandó válasz összeállítása során törekedni kell arra, hogy kizárólag a megkeresés teljesítéséhez (az adatkérés céljához) elengedhetetlenül szükséges személyes adatok átadása valósuljon meg.
69. A nem jogszerű adatkérés teljesítését el kell utasítani. Nem jogszerű a megkeresés, ha a tartalmi vagy alaki feltételek legalább egyike (pl. az adatkérés jogalapja) hiányzik vagy helytelen. Az elutasítással egyidejűleg a hiányzó/helytelen információk pótlását/javítását kell kérni a megkereső szervtől, amennyiben a Társaság részéről a megkeresés teljesítése jogi kötelezettségen vagy jogos érdeken alapulhat. Ha a Lechner Tudásközpont részéről nincs helye az adatátadásnak sem jogi kötelezettség, sem jogos érdek alapján, a jogszerű megkeresést is el kell utasítani.
70. Jogszerű az adatkérés, ha megfelel a tartalmi és alaki feltételeknek, azaz tartalmazza az alábbi információkat:
    a) megkereső szerv pontos megnevezése,
    b) a megkeresés azonosító adatai (pl. iktatószáma, megkeresés alapját képező eljárás száma),
    c) az adatkérés jogalapja (pl. jogszabály és jogszabályhely megjelölése) és feltételei,
    d) az adatkérés célja,
    e) az adatkérés teljesítéséhez, illetve az adatszolgáltatás tárgyának azonosításához szükséges adatok (pl. az érintett személy, tárgy vagy szolgáltatás adatai),
    f) a szolgáltatandó adatok köre, és
    g) az adatszolgáltatás teljesítésének módja és határideje.
71. A nyomozó hatóság személyes adatot, illetve azt tartalmazó tárgyat (pl. irat, filmfelvétel) akkor foglalhat le, ha erről lefoglalási határozatot mutat be. A lefoglalási határozat teljesítését – a törvényesség érdekében – a Jogi Igazgatóság közreműködésével kell végrehajtani. A lefoglalási határozatnak minimálisan az alábbi információkat kell tartalmaznia:
    a) a megkereső nyomozó hatóság pontos megnevezése,
    b) a büntetőeljárás száma,
    c) a lefoglalás tárgya.
72. A szabálysértési eljárást folytató hatóság nem jogosult személyes adatot vagy azt tartalmazó tárgyat (pl. irat, filmfelvétel) lefoglalni.

10 Harmadik országba irányuló adattovábbítás különös szabályai

73. Amennyiben felmerül a személyes adat harmadik országba történő továbbításának szükségessége, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról és feltételeiről.
74. Az adatvédelmi tisztviselő – szükség esetén a Jogi Igazgatóság és az informatikai szakterület véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

11 Adattovábbítás jogos érdek jogalappal

75. A jogos érdek alapján történő adatátadás csak az 6.3. alfejezet szerint lefolytatott érdekmérlegelést követően lehetséges. Az érdekmérlegelés keretében vizsgálni kell a büntető- vagy a szabálysértési eljárás sikeres lefolytatásához fűződő érdeket, amelyet szembe kell állítani az érintett adatvédelmi jogaival. Kizárólag abban az esetben lehet jogszerű az

adatátadás, amennyiben a nyomozó vagy a szabálysértési eljárást folytató hatóság pontosan megjelöli az adatkérés célját és a kért adatkört, mivel ezek feltételei az érdekmérlegelés elvégzésének.

12 Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

76. Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy a Társaság által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.
77. A Lechner Tudásközpont működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos
    a) Informatikai Biztonsági Szabályzat,
    b) Iratkezelési Szabályzat, illetve
    c) általános biztonsági előírásokat tartalmazó szabályzatok.
78. Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi tisztviselőt be kell vonni.
79. Az adatbiztonsági intézkedéseket érintően az adatkezelésért felelős szervezeti egység adatkezelési koordinátora:
    a) a szakterületére vonatkozó információk szolgáltatásával közreműködik az érintett informatikai elemek védelmi osztályokba sorolásában;
    b) a szakterületére vonatkozó információk szolgáltatásával közreműködik az adatkezelés biztonságát fenyegető kockázatok felmérésében és meghatározásában;
    c) az informatikai rendszert üzemeltető szervezeti egységgel együttműködve közreműködik azon információbiztonságot érintő feladatok végrehajtásában, amelyek az adatbiztonsági követelmények megvalósulásához szükségesek;
    d) figyelemmel kíséri a belső adatvédelmi szabályok érvényre juttatását a szakterületen belül, felhívja a szakterületen dolgozók figyelmét a szabályok betartására, jelzi a szabályok megsértését az érintett munkavállaló felettesének, közreműködik a szakterületen dolgozók adatvédelmi tudatosságának növelésében.
80. Az adatbiztonság elveinek egy adatkezelés bevezetésének vagy személyes adatkezelést és/vagy feldolgozást eredményező módosításának előkészítése során történő érvényesítése az informatikai szakterület adatkezelési koordinátorának (megbízottjainak) feladata, aki(ke)t az adatkezelési tevékenységet támogató nyilvántartási rendszerek fejlesztésének, módosításának folyamatába kötelezően be kell vonni.
81. A jelen Szabályzat személyi hatálya alá tartozó személyek kötelesek a személyes adatokat tartalmazó, papíralapon kezelt iratokat a munkavégzés befejezését követően zárt szekrényben, fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik.
82. A Szabályzat személyi hatálya alá tartozó személyek kötelesek a Társaság egyéb belső szabályzatai, így különösen az iratkezelés rendjéről, illetve az általános biztonsági előírásokról szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

83. Az adatbiztonsági intézkedések mindennapi működés során történő betartására a Lechner Tudásközpont minden alkalmazottja, valamint a Társaság informatikai rendszereihez hozzáférő személy köteles.

13 A közös adatkezelői és az adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai

13.1 Közös adatkezelés

84. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit a Lechner Tudásközpont egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk).
85. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen:
    a) az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit;
    b) azt, hogy a közös adatkezelésben érintett egyes adatkezelők mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik;
    c) az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.);
    d) az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.);
    e) az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
    f) az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
    g) az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről;
    h) egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában;
    i) az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;
    j) kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani;
    k) a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.
86. A közös adatkezelés szükségességét az adatkezelési koordinátor az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha a közös adatkezelésről az adatkezelés folyamán születik döntés.
87. Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni – a 10. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatkezelő képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatkezelő nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatkezelővel nem köthető megállapodás közös adatkezelésre.

88. Amennyiben döntés születik a közös adatkezelésről, az illetékes adatkezelési koordinátor(ok) az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő, az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Igazgatóság közreműködésével, továbbá az informatikai szakterület véleményének kikérésével előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit), és azt felterjeszti a szerződés megkötésére jogosult személynek.
89. Az adatkezelési koordinátor a közös adatkezelői megállapodás megkötését követően – az adatkezelési tevékenységek nyilvántartására vonatkozó szabályok szerint – e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Tevékenységek Nyilvántartásában.

13.2 Adatfeldolgozói szerződések

90. Az Adatkezelő az általa kezelt adatok feldolgozására külső adatfeldolgozót abban az esetben vehet igénybe, ha az adatfeldolgozó tevékenysége illetve az adatfeldolgozás során használt rendszer a jelen Szabályzatban meghatározott adatvédelmi és adatbiztonsági követelményeknek, illetve a vonatkozó jogszabályi feltételeknek megfelel.
91. A Társaság fenntartja magának a jogot, hogy tevékenysége során állandó vagy eseti megbízás alapján vegyen igénybe adatfeldolgozót. Állandó jellegű adatfeldolgozásra elsősorban az ügyfélkapcsolattal, a szolgáltatások nyújtásával összefüggő adminisztráció ellátása, valamint az informatikai rendszer fenntartása érdekében kerülhet sor.
92. Adatfeldolgozó igénybevételére kizárólag írásbeli szerződés alapján kerülhet sor.
93. Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni – a 10. fejezet megfelelő alkalmazásával –, hogy a harmadik országbeli adatfeldolgozó képes-e az Általános Adatvédelmi Rendeletnek megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatfeldolgozó nem képes az Általános Adatvédelmi Rendelet által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud ennek megfelelő garanciákat nyújtani a személyes adatok kezelésére, az adatfeldolgozóval nem köthető szerződés.
94. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket az e fejezetben foglalt kiegészítések és pontosítások szerint.
95. Az adatfeldolgozóval kötendő szerződésben:
    a) kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint a Társaság által alkalmazott adatbiztonsági intézkedések, valamint az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;
    b) rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;
    c) rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen

ca/ az adatvédelmi incidens tudomásra jutása esetén a Társaság adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,

cb/ köteles együttműködni a Társaság adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

cc/ köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében;

d) rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

96. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési koordinátor az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

97. Az adatbiztonsági intézkedések technikai megfelelőségének megítélése az informatikai szakterület hatáskörébe tartozik, beleértve azt is, hogy az adatfeldolgozó által egy magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás elegendő garanciát jelent-e az adatbiztonsági szabályok megfelelőségére.

98. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatkezelési koordinátor az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő, az egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi Igazgatóság közreműködésével, továbbá az informatikai szakterület véleményének kikérésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét, és azt felterjeszti a szerződés megkötésére jogosult személynek.

99. Az adatkezelési koordinátor az adatfeldolgozói szerződés megkötését követően – az adatkezelési tevékenységek nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az Adatkezelési Nyilvántartásban.

100. A 90-99. pont rendelkezéseit al-adatfeldolgozó igénybevétele esetén is megfelelően alkalmazni kell azzal, hogy az al-adatfeldolgozó igénybevételére vonatkozó hozzájáruló nyilatkozatnak az adatfeldolgozói szerződés megkötésre jogosult személy általi kiadása előtt az adatkezelési koordinátor kikéri az adatvédelmi tisztviselő és rajta keresztül a Jogi Igazgatóság, továbbá az informatikai szakterület véleményét is.

14 Az Adatkezelési Tevékenységek Nyilvántartása

101. A Lechner Tudásközpont adatkezelői feladatainak segítése keretében az adatvédelmi tisztviselő – az adatkezelési koordinátorok közreműködésével – vezeti az adatkezelési tevékenységek nyilvántartását (Adatkezelési Tevékenységek Nyilvántartása). Az Adatkezelési Tevékenységek Nyilvántartása valamennyi, a Társaság általi adatkezelés esetén tartalmazza:
    a) az adatkezelés célját,
    b) az adatkezelés jogalapját,
    c) az érintettek körét,
    d) az érintettekre vonatkozó személyes adatok kategóriáit,
    e) az adatok forrását (opcionális),

f) az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
h) az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
i) az alkalmazott automatizált döntéshozatali logikákat (opcionális);
j) az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
k) az adatkezelésért felelős szervezeti egység megnevezését és az adatkezelési koordinátor nevét,
l) az adatvédelmi tisztviselő nevét és elérhetőségét,
m) az adatkezelés módszerét (manuális, számítógépes, vegyes),
n) ha lehetséges, az adatbiztonsági intézkedések általános leírását,
o) az archiválás módját, gyakoriságát (opcionális),
p) az érdekmérlegelési teszt és a hatásvizsgálati dokumentum elkészültének tényét.

102. Az Adatkezelési Tevékenységek Nyilvántartásának célja a Lechner Tudásközpont, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.
103. A Társaság adatvédelmi tisztviselője az Adatkezelési Tevékenységek Nyilvántartásába való betekintést – a Hatóság képviselőin kívül – a Lechner Tudásközpont érintett szakterületei, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.
104. Az Adatkezelési Tevékenységek Nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység adatkezelési koordinátora 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az Adatkezelési Tevékenységek Nyilvántartása adatait.
105. Az Adatkezelési Tevékenységek Nyilvántartásával összefüggésben az adatvédelmi tisztviselő:
    a) biztosítja, hogy az adatkezelések bevezetését megelőző döntés előkészítés során az érintett szakterületek az Adatkezelési Tevékenységek Nyilvántartása adatait megismerhessék a felesleges, párhuzamos adatkezelések elkerülése, illetve az új adatkezelésnek a meglévő adatkezelésekhez való illeszkedése érdekében;
    b) ellenőrzi az adatkezelések, közös adatkezelők, illetve adatfeldolgozók adatainak az Adatkezelési Tevékenységek Nyilvántartásába történő rögzítését, és jelzi az adatkezelésért felelős szervezeti egység vezetőjének a hiányos, hibás vagy valószínűleg megváltozott adatokat, információkat;
    c) a Jogi Igazgatósággal együttműködve figyelemmel kíséri az adatkezelést érintő jogszabályok változását és a szükséges módosításokra felhívja az adatkezelési koordinátorok figyelmét;
    d) a Hatóság megkeresésére adatot szolgáltat az Adatkezelési Tevékenységek Nyilvántartásából.

15 Az adatvédelmi incidensek kezelése

15.1 Rendkívüli esemény (adatvédelmi incidens) bejelentése

106. Az a munkavállaló, aki a Lechner Tudásközpont által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy a Társaság szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban rendkívüli eseményt (adatvédelmi incidenst vagy annak gyanúját) észleli, köteles azt haladéktalanul bejelenteni az [info@lechnerkozpont.hu] e-mail címen. Az előbbieken túli, egyéb bejelentő Társaság elektronikus elérhetőségén jelentheti be a rendkívüli eseményt, illetve az adatvédelmi incidenst vagy annak gyanúját.
107. Az Általános Adatvédelmi Rendeletben foglaltak alapján az adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
108. Ha a rendkívüli esemény felveti az adatvédelmi incidens gyanúját, akkor a bejelentésben ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az adatvédelmi incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát, továbbá a bejelentő nevét és elérhetőségét.
109. A rendkívüli esemény bejelentésével egyidejűleg meg kell tenni azokat a szükséges és haladéktalan intézkedéseket, amelyek a rendkívüli esemény jellegéből következnek (pl. áramtalanítás, katasztrófaelhárítók értesítése, terheléses támadás blokkolása), s a káros jelenség megszakítását, a lehetséges károk csökkentését célozzák. A haladéktalan intézkedéseket lehetőleg úgy kell megtenni, hogy a rendkívüli esemény kivizsgálásához szükséges bizonyítékok megmaradjanak.

15.2 Incidens esetén követendő eljárás

110. A rendkívüli esemény (papíralapú és nem papíralapú adatokra vonatkozóan egyaránt) 15.4. fejezetnek megfelelő kivizsgálását és a 1207. pont szerinti kategorizálását, valamint a haladéktalanul megteendő intézkedések meghatározását az incidensvizsgáló bizottság végzi. Az incidensvizsgáló bizottság tagjai: a Lechner Tudásközpont adatvédelmi tisztviselője, azon szakterület képviselője ahol az incidens történt, és az információbiztonsági vezető. Az incidensvizsgáló bizottság a rendkívüli esemény jellegének megfelelően további tagokkal bővíthető. Egyszerű elbírálású ügyekben az incidensvizsgáló bizottság összehívása mellőzhető, az adatvédelmi tisztviselő önállóan jár el.
111. Az incidensvizsgáló bizottságot az adatvédelmi tisztviselő hívja össze. Az incidensvizsgáló bizottság tagjainak – szükség esetén – munkaidőn kívül is rendelkezésre kell állniuk. Az incidensvizsgáló bizottság munkáját az adatvédelmi tisztviselő koordinálja, és képviseli a Társaság egyéb szervezeti egységei felé.
112. Az incidensvizsgáló bizottság döntéseiről indoklást is tartalmazó feljegyzést kell készíteni. Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére a Lechner Tudásközpont mindenkori iratkezelési szabályai az irányadók. Az incidensvizsgáló bizottság korlátozhatja a munkájáról szóló dokumentumokba betekintők körét (ide nem értve az ügyvezetőt).
113. Az adatvédelmi incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az adatvédelmi incidens vizsgálatának lezárásától számított 10 évig, illetéktelenek számára hozzá nem férhető, zárt helyen kell megőrizni.
114. Az adatvédelmi incidensről az adatvédelmi tisztviselő a Jogi Igazgató útján értesíti az ügyvezetőt, valamint – az esetlegesen szükséges egyéb szervezeti egységeket.

115. Az informatikai szakterületnek a riasztásokban szereplő sérülékenység esetén a következők szerint kell eljárni:
    a) figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
    b) amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell;
    c) amennyiben a Társaság rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
    d) ha a Lechner Tudásközpont nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
    e) amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.
116. A nem papíralapon kezelt adattal kapcsolatos adatvédelmi incidensek kezelésére a Lechner Tudásközpont a mindenkor hatályos Informatikai Szabályzatában foglaltak is irányadóak.
117. A rendkívüli eseményt előzetes kivizsgálás keretében kategóriába kell sorolni (adatvédelmi incidens, információbiztonsági incidens, általános biztonsági incidens).
118. A Hatóságnak történő bejelentés határidejének számítása szempontjából az adatvédelmi incidensről tudomásszerzés időpontja az az időpont, amikor a rendkívüli eseményt az incidensvizsgáló bizottság adatvédelmi incidens kategóriába sorolja.
119. A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről a 1066. pontban meghatározott elérhetőségen a Lechner Tudásközpont adatvédelmi tisztviselőjét köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

15.3 Az adatvédelmi incidens minősítése

120. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések akár vétlen, akár szándékos megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:
    a) súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl. a jogosulatlan hozzáférés során megismert adatok, olyan adatsérülés, adatvesztés, amelynél az adatok naplózott adatállományból, biztonsági mentésből nem állíthatóak helyre).
    b) magas kockázatú incidens: az az incidens, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek (pl. az érintett személyes adatai feletti rendelkezési jogának elvesztését vagy jogai korlátozását, hátrányos megkülönböztetést, személyazonosság-lopást vagy a személyazonosságával való visszaélést, pénzügyi veszteséget, jó hírnevének sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését eredményezheti);
    c) enyhe incidens: minden incidens, amely nem tartozik az a)-b) pont alá (pl. átmeneti szolgáltatásleállás, illetve kiesés a Társaság munkavállalói által használt belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

121. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni a Lechner Tudásközpont tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt személyes adatokra, továbbá a Társaság alkalmazottainak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt személyes adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat a Lechner Tudásközpont birtokában lévő papíralapú adathordozón lévő személyes adatokra is alkalmazni kell.
122. Az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli esemény egyúttal adatvédelmi incidensnek is minősül, amennyiben személyes adatokra nézve következik be. A jelen Szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

15.4 Az adatvédelmi incidens kivizsgálása

123. A rendkívüli eseményről (adatvédelmi incidensről vagy annak gyanújáról) szóló bejelentés megvizsgálása során az alábbi szempontokat kell figyelembe venni:
    a) a bejelentés személyes adatot érint-e;
    b) amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre;
    c) megállapítható-e az incidensben érintett személyek köre;
    d) a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt;
    e) az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve;
    f) melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények;
    g) a Társaság által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.
124. A bejelentőt – szükség esetén – további információk közlésére kell felkérni.
125. Ha az incidens bejelentés előzetes megvizsgálása azzal az eredménnyel jár, hogy az elektronikus információs rendszereket érintő (informatikai biztonsági vagy általános biztonsági) rendkívüli esemény nem érintett személyes adatokat, akkor a vizsgálatot a Lechner Tudásközpont mindenkor hatályos Informatikai Biztonsági Szabályzatában foglaltak, illetve a Társaság működési rendje szerint kell tovább folytatni.
126. Az incidensvizsgáló bizottság – adatvédelmi incidens esetén az adatvédelmi tisztviselő útján – legkésőbb a rendkívüli esemény bejelentését vagy a rendkívüli esemény adatvédelmi incidens kategóriába sorolását (tudomásszerzés) követő 1 naptári napon belül tájékoztatja a következő személyeket a bejelentésben foglaltakról vagy az előzetes vizsgálat eredményéről, továbbá a Hatóságnak történő bejelentés szükségességéről, valamint arról, hogy szükséges-e a rendkívüli esemény (adatvédelmi incidens) részletes vizsgálata:

a) a Lechner Tudásközpont ügyvezetőjét;
b) jogi igazgatót;
c) informatikai rendszert is érintő rendkívüli esemény esetén az informatikai szakterület vezetőjét;
d) az incidenssel érintett, szakmailag illetékes szervezeti egység vezetőjét.

127. Az incidensvizsgáló bizottság javaslata alapján az ügyvezető legkésőbb a bizottság javaslatának kézhezvételét követő 1 naptári napon belül dönt a Hatóságnak történő bejelentés szükségességéről.
128. Az adatvédelmi incidens részletes vizsgálatának szükségességéről az incidensvizsgáló bizottság dönt. A részletes vizsgálatot legkésőbb a döntést követő naptári napon meg kell kezdeni, s a vizsgálat megkezdésének napjától számított legfeljebb 15 munkanapon belül le kell zárni.
129. Az adatvédelmi incidens részletes vizsgálata során elsősorban az alábbi módszerek alkalmazhatóak:
    a) személyes megbeszélés az adatvédelmi incidenst észlelő személyekkel, valamint az érintett szervezeti egységek munkatársaival és vezetőivel;
    b) írásbeli tájékoztatás kérése az érintett szervezeti egységektől;
    c) dokumentumok vizsgálata;
    d) informatikai rendszerek, hálózatok és eszközök vizsgálata.
130. Amennyiben az incidensvizsgáló bizottság a részletes kivizsgálás eredményei alapján úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az adatvédelmi incidenssel azonos problémaforrásból eredő újabb incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja az érintett szervezeti egységek vezetőit.
131. Az incidensvizsgáló bizottság a részletes vizsgálat megállapításairól, illetve a javasolt intézkedésekről a részletes vizsgálat befejezését követő 2 munkanapon belül vizsgálati jelentést készít. A vizsgálati jelentés tartalmazza az adatvédelmi incidens elhárításához és további incidens megelőzéséhez szükséges intézkedésekre vonatkozó, az illetékes vezető részére tett javaslato(ka)t is.
132. A részletes vizsgálatról szóló jelentést a 126. a)-d) alpontjaiban említett vezetőknek kell megküldeni.
133. Az adatvédelmi incidens elhárítása, valamint a további adatvédelmi incidensek megelőzése céljából megtett egyes intézkedésekről az adatvédelmi incidenssel érintett szervezeti egység vezetője tájékoztatást küld az adatvédelmi tisztviselő részére.

15.5 Az érintett tájékoztatása a súlyos adatvédelmi incidensről

134. Súlyos adatvédelmi incidens esetén a Lechner Tudásközpont – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (vö. GDPR 34. cikk) a Társaság honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
135. Az érintett részére adott tájékoztatásban egyértelműen és közérthetően ismertetni kell az adatvédelmi incidens jellegét, valamint közölni kell legalább az alábbi információkat és intézkedéseket:
    a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
    b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

c) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

15.6 Az érintettet nem kell tájékoztatni, ha az adatvédelmi incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:

a) a Társaság megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket (pl. titkosítás alkalmazása), amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) a Társaság az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan intézkedést kell tenni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

136. Az ügyvezető döntése alapján a Lechner Tudásközpont az érintetteket a Társaság honlapján vagy országos lefedettséggel rendelkező sajtótermékben közzétett hirdetmény útján is értesítheti.

15.7 Az adatvédelmi incidens bejelentése a Hatóságnak

137. Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni.

138. Az adatvédelmi incidens bejelentése összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

139. Ha nem lehetséges az bejelentéshez szükséges információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később, részletekben is közölhetők.

15.8 Az Adatvédelmi Incidensek Nyilvántartása

140. Az adatvédelmi incidensekről az adatvédelmi tisztviselő elektronikus nyilvántartást (Adatvédelmi Incidensek Nyilvántartása) vezet.

141. Az Adatvédelmi Incidensek Nyilvántartásában rögzíteni kell:

a) az adatvédelmi incidensben érintett személyes adatok körét és számát,

b) az adatvédelmi incidenssel érintettek körét és számát,

c) az adatvédelmi incidens észlelésének és tudomásszerzésének (adatvédelmi incidens kategóriába sorolásának) időpontját,

d) az adatvédelmi incidens körülményeit, lehetséges és bekövetkezett hatásait,

e) az adatvédelmi incidens elhárítására megtett intézkedéseket,

f) az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait,

g) a Hatósághoz történt bejelentés adatait.

16 Belső adatvédelmi felülvizsgálati eljárás

142. A Lechner Tudásközpont szervezetén belüli adatvédelmi felülvizsgálati eljárás (a továbbiakban: belső adatvédelmi ellenőrzés) célja, hogy az adatvédelmi tisztviselő meggyőződjön arról, hogy a Társaság egyes szervezeti egységei az adatvédelemmel

kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e a személyes adatokat.

143. Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves adatvédelmi ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét, az ellenőrzés várható időpontját és az ellenőrzés tárgykörét kell tartalmaznia. Az éves adatvédelmi ellenőrzési terveket úgy kell összeállítani, hogy négyéves időtartam alatt lehetőség szerint minden, adatkezelésért felelős szervezeti egység ellenőrzésére sor kerüljön. Az éves adatvédelmi ellenőrzési tervet legkésőbb az adott év február 28. napjáig kell elkészíteni, és a Társaság ügyvezetője részére bemutatni.
144. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi tisztviselő a javasolt időpontban megkezdhesse a belső adatvédelmi ellenőrzést, illetve szükség esetén – az adatvédelmi tisztviselő által javasolt időponthoz képest legfeljebb tíz munkanapon belüli – új időpontra tesz javaslatot.
145. A belső adatvédelmi ellenőrzés során az adatvédelmi tisztviselő a szervezeti egység irodahelységeibe beléphet, a szervezeti egység – a belső adatvédelmi ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet.
146. Az adatvédelmi tisztviselő a lefolytatott belső adatvédelmi ellenőrzés megállapításairól vizsgálati jelentést készít.
147. Ha az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályzatoknak vagy jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. Az adatvédelmi tisztviselő javaslata alapján megtett intézkedésekről a szervezeti egység vezetője tájékoztatja az adatvédelmi tisztviselőt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni (utóellenőrzés). Az utóellenőrzésre a 144-146. pontban foglaltakat alkalmazni kell.
148. Az adatvédelmi tisztviselő rendkívüli belső adatvédelmi ellenőrzést is lefolytathat, ha az adatvédelmi szempontból indokolt, különösen, ha a személyesadat-kezeléssel érintettek száma jelentős. Rendkívüli belső adatvédelmi ellenőrzésnek minősül az éves adatvédelmi ellenőrzési tervben nem szereplő belső adatvédelmi ellenőrzés. A rendkívüli belső adatvédelmi ellenőrzésre a 145-146. pont rendelkezéseit alkalmazni kell.
149. Az adatvédelmi tisztviselő a belső adatvédelmi ellenőrzés (ideértve a 147. pont szerinti utóellenőrzést is) lefolytatását követően tájékoztatja a Társaság ügyvezetőjét a belső adatvédelmi ellenőrzés adatairól és eredményeiről. Az ügyvezető tájékoztatása történhet szóban vagy a vizsgált szervezeti egység vezetője által elfogadott, 146. pont szerinti vizsgálati jelentés megküldésével is.
150. Az adatvédelmi tisztviselő a Lechner Tudásközpont adatvédelmi helyzetéről szóló éves jelentésnek tartalmaznia kell az adott évben lefolytatott belső adatvédelmi ellenőrzésekkel és utóellenőrzésekkel kapcsolatos összegző információkat és megállapításokat, valamint a vizsgált szervezeti egység által megtett intézkedéseket is.