ADATVÉDELMI

SZABÁLYZAT

TARTALOMJEGYZÉK

1. Az Adatvédelmi Szabályzat (továbbiakban: Szabályzat) célja

1.1. A **TREZOR Záloghitelező Zártkörűen Működő Részvénytársaság** (székhely: 1165 Budapest, Kardosfa utca 12. A. ép. 4. ajtó, a továbbiakban: „**Társaság**") belső ellenőrzési rendszerének – **belső védelmi vonalainak** - elemei az adatok védelmének biztosítása. A szabályzat célja az adatok és egyes erőforrások biztonság-érzékenysége megállapításának szabályozása annak érdekében, hogy kezelésük, illetve alkalmazásuk során a biztonság érzékenységükkel arányos erősségű védelmet határozzanak meg számukra.

2. A Szabályzat tárgya

2.1. A jelen szabályzat tárgya az adatok, információk biztonságos kezelésének szabályozása. Egyes adatok, információk biztonságos kezelésének rendjét az Informatikai Biztonsági Szabályzat, Iratkezelési Szabályzat, valamint az Leltározási és Selejtezési Szabályzat is szabályozza. Az ott szabályozott kérdésekben az Informatikai Biztonsági Szabályzat, Iratkezelési Szabályzat, valamint az Leltározási és Selejtezési Szabályzat rendelkezéseit kell használni.

2.2. Jelen szabályzat tárgya továbbá az adatok, és egyes erőforrások biztonság érzékenységének biztonsági fokozatonkénti megállapítása.

3. A Szabályzat hatálya

3.1. A Szabályzat tárgyi hatálya kiterjed a Társaság valamennyi, alanyi hatály alá tartozó személy (munkavállaló, alvállalkozó, stb) által folytatott valamennyi adatra, számítógépes és manuális adatkezelésre, illetve adatfeldolgozásra.

3.2. A Szabályzat alanyi hatálya kiterjed a Társaság

a.) munkaviszony alapján foglalkoztatott munkatársaira,
b.) szerződéses jogviszony alapján munkafeladatot végrehajtókra,
c.) vezető tisztségviselőkre,
d.) titoktartási nyilatkozat aláírását követően munkafeladatot végrehajtókra.

3.3. A Szabályzat időbeli hatálya aláírásától módosításáig, visszavonásáig terjed

4. Jelen Szabályzat során alkalmazott fogalmak meghatározása:

Az adat tények, elképzelések, utasítások formalizált ábrázolása ismertetés, (tovább) feldolgozás, illetve távközlés céljára. (a személyes adatok, az adatok egy részét képezik).
Az információ fogalma az adat fogalmával megegyezik.
Az adatkezelés az alkalmazott eljárástól függetlenül az adatok felvétele, tárolása, hasznosítása, továbbá adatkezelésnek minősül az adatok megváltoztatása, és a további felhasználás megakadályozása is.
Eszköz a hardver, rendszer szoftver, alkalmazói szoftver, vagy más az adatok manuális vagy gépi kezelését, és az erőforrások kiszolgálását szolgáló berendezés (pl. papír, és elektronikus adathordozók, sokszorosító gép, légkondicionáló berendezés, felvonó).
Az adatvédelem a személyes adatok jogszabályoknak, és a Társaság belső szabályainak megfelelő védelmének szabályozása.
Az adatbiztonság az adatok bizalmasságának, sértetlenségének, és/vagy rendelkezésre állásának minimális fenyegetettsége.
Az osztályozás az adatok, és egyes erőforrások biztonság érzékenységének megfelelő biztonsági osztályokba sorolása. (osztályba sorolás).
Adatvédelmi felelős az SZMSZ-ben megjelölt adatvédelmi felelős.
Adatgazda A Társaság adatgazdája az SZMSZ-ben megjelölt személy.

Szigorúan titokban tartandó adat: minden olyan az olyan adat, tény, információ, amely banktitkot, üzleti titkot, szolgálati titkot, vagy személyes adatot tartalmaz, és amelyeknek jogosulatlan harmadik személy általi illetéktelen megszerzése a Társasággal szembeni hatósági eljárás alapját képezheti.
Kiemelten védendő titok: Kiemelten védendő titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság, **prudens tevékenységét** megakadályozná, vagy súlyosan veszélyeztetné.
Védendő jelentős titok: Védendő jelentős titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság jogos érdekeit **súlyosan** sértené, vagy súlyosan veszélyeztetné, de a prudens működést nem korlátozza vagy veszélyezteti.
Védendő titok: Védendő titoknak minősül az olyan adat, tény, információ, amelynek illetéktelen személy tudomására jutása a Társaság érdekeit enyhébb fokban sértené, vagy veszélyeztetné.

5. Védendő adat és titok a Társaságnál

5.1. Banktitok

Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.

5.2. Üzleti titok

Az üzleti titok fogalma alatt a Polgári Törvénykönyvről szóló 2013. évi V. törvényben meghatározott fogalmat kell érteni.

5.3. Szolgálati titok

Minden olyan, a Társaság tevékenységéhez kapcsolódó tény, információ, megoldás vagy adat, amelynek a titokban maradásához a Társaságnak méltányolható érdeke fűződik, és amely információ, adat nem szerepel közhiteles nyilvántartásban, illetve amely nem kerül közzétételre.

5.4. 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;

6. A biztonsági osztályozás

6.1. Adatok osztályozása

Adatok osztályozása bizalmasság, sértetlenség és rendelkezésre állás alapján történik A, B, C és D osztályokba a következő követelményrendszer alapján:

BIZALMASSÁG A rendszer biztonsági mechanizmusai biztosítják, hogy a rendszerben kezelt vagy a számítógépes hálózaton továbbított adat, információ a jogosulatlanok számára ne legyen elérhető, vagy véletlenül se kerüljön nyilvánosságra, azaz ne történjen jogosulatlan információszerzés.		
Kategória	Definíció	Követelmények
A	**Igen Kritikus** minden olyan fontos tény, információ, adat és megoldás, amelynek titokban maradásához a	Az B kategóriájú követelményeken felül

	Társaságnak és partnereinek méltányolható érdeke fűződik, és amelyet üzleti titokká minősített. Hozzáférés kizárólag a felső szintű vezetők (Elnök-Vezérigazgató, Tulajdonosok) engedélyével történhet.	titkosítási megoldást kell alkalmazni az adatok tárolása, illetve továbbítása során.
B	**Kritikus** melynek szervezeten belüli nyilvánosságra kerülése legalább jelentős kár, tartalmát kizárólag adott szakterületek ismerhetik meg (pl. személyes adatok, ügyfelek adatai stb.).	A C kategóriájú követelményeken felül csoportszintű jogosultságokkal szükséges biztosítani a védendő adatok bizalmasságát.
C	**Nem kritikus I** adat, melynek társadalmi nyilvánosságra kerülése legalább jelentős kár és szervezeten belüli nyilvánosságra kerülése elhanyagolható, tartalmát kizárólag a Társaság munkavállalói ismerhetik meg.	Csak a Társaság felhasználója kaphat hozzáférést az adathoz. Felhasználó hitelesítés szükséges.
D	**Nem kritikus II.** adat, melynek nyilvánosságra kerülése elhanyagolható, a Társaság érdekeit semmilyen módon nem sérti.	Nincs meghatározott követelmény

SÉRTETLENSÉG

A rendszer biztonsági mechanizmusai biztosítják, hogy az adatot, információt vagy programot csak az arra jogosultak változtathatják meg, illetve azok észrevétlenül nem módosulhatnak.

Kategória	Definíció	Követelmények
A	Kritikus adat, melynek illetéktelen törlése vagy módosítása legalább súlyos kár	Az B kategóriájú követelményeken felül az Elnök-Vezérigazgató szintje alatt alkalmazni kell a négy-szem elvet az adatok módosítása során.
B	Nagyon fontos adat, melynek illetéktelen módosítása legalább jelentős kár.	A C kategóriájú követelményeken felül csoport szintű jogosultságokkal szükséges biztosítani a védendő adatok bizalmasságát, továbbá az adatok nem kívánt módosítása érdekében az adathoz való írási jogot csak korlátozott számú felhasználó kaphat.
C	Fontos adat, melynek illetéktelen törlése legalább jelentős kár.	Felhasználó hitelesítés szükséges.
D	Nem fontos adat, mely hitelességének sérülése elhanyagolható kár.	Nincs meghatározott követelmény

RENDELKEZÉSRE ÁLLÁS

Az a tényleges állapot, amikor az adatok állandóan, illetve egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva

Kategória	Definíció	Hibamentesség	Maximum kiesési idő	Maximális adatvesztési követelmények
A	Folytonos	99,98	2 óra	12 óra

B	Folytonos	99 %	12 óra	24 óra
C	Növelt redundancia	97,5 %	24 óra	1 hét.
D	Redundancia	95 %	1 hét	Nincs meghatározott követelmény

Adatok végső biztonsági osztálya a bizalmasság, sértetlenség és rendelkezésre állás alapján megjelenő osztályok közül (A, B, C, D) a legmagasabb.

6.4. Az egyes osztályok szerinti besorolásokat az 1. számú mellékletként csatolt Titokköri Jegyzék tartalmazza.

7. Biztonsági osztályozás folyamata

- Adat, információ, osztályozása az érintett területet a Társaság Szervezeti és Működési Szabályzata (SZMSZ) szerinti adatvédelmi felelős kötelezettsége.
- Az Adatvédelmi felelős leltárba veszi a Társaság által kezelt teljes adatállományt.
- Az Adatvédelmi felelős az előző fejezet meghatározási alapján osztályba sorolja az adatokat
- Az Adatvédelmi felelős meghatározza, hogy az adatok kezelése milyen épületekben, helyiségekben történik. Minden helyiség az ott kezelt adatok biztonsági osztályát kapja.
- Az Adatvédelmi felelős meghatározza, hogy az adatok kezelése milyen eszközökkel történik. Minden eszköz (hardver, szoftver stb.) az általa kezelt adatok biztonsági osztályát kapja.

Adat, információ helyiség biztonsági osztályozását a keletkezésekor, illetőleg a Társaság általi birtokbavételkor kell elvégezni jelen szabályzat alapján.

Adat, információ, helyiség, rendszer biztonsági besorolásának módosítására a besorolást végző adatvédelmi felelős, illetőleg az ügyvezető jogosult.

Titokköri jegyzék módosítására az adatvédelmi felelős – a besorolásra jogosult adatgazda kezdeményezésére – jogosult.

8. A biztonság érzékeny erőforrások védelme

8.1. A védelem tárgya

8.1.1. A védelem tárgya az erőforrások **bizalmassága,** azaz a felfedés elleni védelmük, a **sértetlensége**, azaz a módosítás elleni védelmük, és a **rendelkezésre állásuk**, azaz a megsemmisülésük (eltulajdonításuk) elleni védelmük. A kontrol (védelmi) intézkedéseket a biztonsági szabályozások tartalmazzák.

8.2. A védelem erőssége

Szükséges, hogy a védelem erőssége, – amelyet a biztonsági osztályba sorolás szerint a biztonsági szabályozásokban rendelnek hozzájuk, – az A osztályban a legerősebb legyen, és attól lejjebb fokozatosan gyengüljön.

9. Az adatok, és egyéb erőforrások kezelésének rendje

9.1. A biztonsági osztályozás megőrzése

Az adatoknak a biztonsági osztályozásukat meg kell őrizni az adathordozó (papír vagy elektronikus) változásától függetlenül.

9.2. A tárolás, üzemeltetés, karbantartás rendje:
Az osztályozott helyiségek nem nyílhatnak az osztályozásukkal csak azonos osztályozású vagy egy osztállyal alacsonyabb/magasabb osztályozású helyiségből.

9.3. Az eszközök osztályozása a tárolt adatok, alkalmazások szerint:
Az eszközök, amennyiben osztályozott adatot, szoftvert, alkalmazást tárolnak (pl. notebook) maguk is osztályozottak, és az osztályozással megegyező módon kell kezelni őket.

9.4. A selejtezés
Az osztályozott erőforrásokat a Leltározási és Selejtezési Szabályzat szerint kell selejtezni.

10. Az adatvédelmi felelős

10.1. Szervezeti elhelyezkedése:
Az adatvédelmi felelős olyan munkaviszony, vagy tartós megbízási jogviszony alapján foglalkoztatott munkatárs, aki az ügyvezető közvetlen alárendeltségébe tartozik.

10.2. Az adat-, és titokvédelmi felelős feladatai különösen:

- Releváns jogszabályok módosításának követése, a szabályzaton történő átvezetésének kezdeményezése,
- A Szabályzat naprakészen tartása, és az egyes változatokról, módosításokról a munkatársak tájékoztatása.
- A titokköri jegyzékbe felvétel, és törlés az adatfelelősök illetőleg az ügyvezető állásfoglalásai alapján, figyelembe véve a Szabályzatot.
- A Szabályzat előírásai végrehajtásának felügyelete.
- A Szabályzat végrehajtásával kapcsolatban keletkező jegyzőkönyvek archiválása.
- A biztonsági szabályozások készítőivel, karbantartóival konzultáció, a Szabályzat hatályosítása érdekében.
- A Szabályzat hatókörébe tartozó biztonsági események esetén, a Szabályzat alapján az esemény osztályozása.
- A Szabályzat felső vezetőknek történő oktatásának előkészítése, megszervezése. Az oktatásról jelenléti ív, és a hallgatók tudomásul vételi nyilatkozatának felvétele, megőrzése
- Az új belépő munkatársak oktatása
- Évente legalább egy alkalommal felülvizsgálni a Szabályzat rendelkezéseit.

11. Elsődlegesen figyelembe vett jogszabályok, szabványok

Jogszabályok

- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE 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 (általános adatvédelmi rendelet)

Szabványok

- MSZ ISO/IEC 27001:2022 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények Magyar Szabvány
- FIPS PUB 140-3. Security Requirements for Cryptographic modules. March 22, 2019 NIST,

12. A szabályzat hatályba lépésének időpontja:

Az adatvédelmi szabályzat az aláírás napján lép hatályba.

Budapest, 2025. május 29.

……..
Igazgatóság nevében
Igazgatósági tagok együttesen

Mellékletek

1. Titokköri jegyzék és függeléke

1. sz. Melléklet

TITOKKÖRI JEGYZÉK

Hatályos: módosításáig

1. ADATOK

1.1. Szigorúan titkos adatok (amelyek vagy Banktitkot, vagy üzleti titkot képeznek, „A" osztály)

- Arra jogosult által ilyen osztályba sorolt adatok;
- A Társasággal szerződésben álló pénzügyi intézmények és más szervezetek kezelésre átadott, banktitkot képező adatai;
- A nem pénzügyi intézményektől kezelésre átvett adatok;
- A Társaság szerződéses ügyfeleinek adatai, az ügyfelek listája;
- Üzleti folyamatok kockázati mátrixai;
- Belső ellenőrzés ütemtervei és jelentései;
- Minőségbiztosítás adatai;
- Tervezetek, munkaanyagok;
- Alkalmazott szoftverek dokumentációja;
- Jogi adatok;
- A pénzügyi, számviteli adatok;
- Kontrolling adatok;
- Társaság archivált adatai;
- Banki szoftver és a hozzá kapcsolódó adatbázis;

1.2. Titkos adatok (Személyes adatok, „B" osztály)

- Arra jogosult által ilyennek sorolt adatok;
- Informatikai Biztonsági Szabályzat;
- A naplók adatai (audit trail, audit log, behatolási log a fizikai belépés ellenőrzés adatai, a biztonsági felügyelet naplója);
- A Társaság munkatársai személyi anyagai (munkaszerződések, önéletrajzok, bizonyítványok stb.);
- A munkatársak humánpolitikai adatai;
- A bérlisták;
- A harmadik felek szerződés alapján a Társaság területén feladatot teljesítő munkatársainak adatai;
- Felügyeleti intézkedések, határozatok;
- Az Igazgatósági, Felügyelő Bizottsági ülések anyagai;
- Szervezeti Működési Szabályzat;
- Telefonjegyzék;
- Fájl szerveren tárolt dokumentumok;

1.3. Bizalmas adatok („C" osztály)

- Arra jogosult által ilyennek sorolt adatok;
- Közgyűlési anyagok;
- Vezetői értekezletek anyagai;
- Cégiratok;

- Az „A” és „B” osztályba nem sorolt informatikai biztonsági szabályozások, valamint az Adatvédelmi Szabályzat;
- Belső ellenőri szabályozások, a mellékleteket kivéve;
- Társaság szolgáltató, illetve szállító partnerei szerződései;
- Marketing tervek, programok;
- Levelező rendszer;

1.4. Nem osztályozott adatok („D” osztály)

- Közzétételre készített mérleg-, és cégadatok;
- Reklám, és propagandaanyagok;
- Oktatási anyagok;
- Vállalati stratégia;
- Üzleti, és Informatikai Stratégia;

2. ALKALMAZÁSOK, ÜZLETI FOLYAMATOK

A 6. pontban megadott osztályozásnak megfelelően besorolva

Üzleti folyamatok („A” osztály)

- Az üzleti folyamatokat kiszolgáló informatikai alkalmazások;

Támogató folyamatok („B” osztály)

- Erőforrások üzemeltetése;
- Szabványosítás;
- Értékesítés, marketing;
- Pénzügy;
- Bérszámfejtés;
- Jogi képviselet;
- Minőségbiztosítás;
- Kontrolling;
- Vállalatirányítás;
- Humán erőforrás gazdálkodás;
- Belső ellenőrzés;

3. HELYISÉGEK

Zárt helyiségek („A” osztály)

Kiemelten ellenőrzött helyiségek („B” osztály)

- Belső ellenőr irodája
- Központi hálózati eszközöket tartalmazó helység
- Ellenőrzött helyiségek („C” osztály)
- A Kiemelten ellenőrzött helyiségek osztályban fel nem sorolt irodák, tanács-, és oktató termek

Nem osztályozott helyiségek („D” osztály)

- Ügyfélfogadó (Recepciók előterei)

4. ESZKÖZÖK

Szigorúan titkos eszközök („A” osztály)

- Számítástechnikai eszközök, ha osztályozott anyagot tárolnak, kezelnek
- A naplók

Nem osztályozott eszközök („C” osztály)

- Minden egyéb eszköz

5. ADATVAGYON ÉS TÁMOGATÓ INFORMATIKAI RENDSZEREK BESOROLÁSA

Az adatvagyon elemek és az őket támogató informatikai rendszerek osztályozását (bizalmasság, sértetlenség, és rendelkezésre állás) az **Adatgazda** végzi az alábbiak szerint:

5.1. Bizalmasság szerinti osztályozás

5.1.1. Igen Kritikus („A” osztály – megőrzési idő: 10 év)

- Arra jogosult által ilyen osztályba sorolt adatok;
- A Társasággal szerződésben álló pénzügyi intézmények és más szervezetek kezelésre átadott, banktitkot képező adatai;
- Alkalmazott szoftverek;
- Banki szoftver és a hozzá kapcsolódó adatbázis;
- A naplók adatai (audit trail, audit log, behatolási log a fizikai belépés ellenőrzés adatai, a biztonsági felügyelet naplója);
- A munkatársak humánpolitikai adatai;
- A bérlisták;
- A harmadik felek szerződés alapján a Társaság területén feladatot teljesítő munkatársainak adatai;
- Szervezeti Működési Szabályzat;
- Telefonjegyzék;
- Fájl szerveren tárolt dokumentumok;
- Levelező rendszer;

5.1.2. Kritikus („B” osztály – megőrzési idő: 15 év)

- Arra jogosult által ilyen osztályba sorolt adatok;
- Az Igazgatósági, Felügyelő Bizottsági ülések anyagai;
- Belső ellenőri szabályozások, a mellékleteket kivéve;
- A nem pénzügyi intézményektől kezelésre átvett adatok;
- Jogi adatok;
- A Társaság munkatársai személyi anyagai (munkaszerződések, önéletrajzok, bizonyítványok, stb.);
- Belső ellenőrzés ütemtervei és jelentései;
- Társaság archivált adatai;
- A Társaság szerződéses ügyfeleinek adatai, az ügyfelek listája;
- Társaság szolgáltató, illetve szállító partnerei szerződései;

5.1.3. Nem kritikus I. („C” osztály – megőrzési idő: 8 év)

- Arra jogosult által ilyen osztályba sorolt adatok;
- Adatvédelmi Szabályzat;
- Tervezetek, munkaanyagok;
- Üzleti folyamatok kockázati mátrixai;

- Minőségbiztosítás adatai;
- Informatikai Biztonsági Szabályzat;
- Oktatási anyagok;
- Vállalati stratégia;
- Közgyűlési anyagok;
- Vezetői értekezletek anyagai;
- Üzleti, és Informatikai Stratégia;
- Kontrolling adatok;
- A pénzügyi, számviteli adatok;
- Marketing tervek, programok;

5.1.4. Nem Kritikus II („D" osztály – megőrzési idő nem korlátozott)

- Arra jogosult által ilyen osztályba sorolt adatok;
- Nyilvános ÁSZF és ÜSZ;
- Kondíciós listák és hirdetmények;
- Közzétételre készített mérleg-, és cégadatok;
- Reklám, és propagandaanyagok;
- Nyilvános cégiratok;
- Nyilvánosságra került felügyeleti intézkedések, határozatok;

5.2. Sértetlenség szerinti osztályozás

5.2.1. Kritikus („A" osztály)

- Székhely betörésvédelmi funkciói;
- Internet szolgáltatás;
- Banki szoftver és a hozzá kapcsolódó ügyfél-adatbázis;
- Felhasználói számítógépek;
- A naplók adatai (audit trail, audit log, behatolási log a fizikai belépés ellenőrzés adatai, a biztonsági felügyelet naplója);
- tartalékberendezések,
- Vírusvédelmi programok installálása során ajánlott a kritikus rendszerfájlok és információk;
- Tűzfal, switch;
- Az üzleti kapcsolattal összefüggésben keletkezett iratokról (pl. üzleti levelezések), azok másolatai;
- Az FIU megkeresései alapján tett intézkedések.

5.2.2. Nagyon fontos („B" osztály)

- az ügyfél-átvilágítás során felvett (beleértve az elektronikus azonosítás során keletkezett) személyes adatok, ideértve a pénzeszköz és vagyon forrására vonatkozó információkat,
- nem személyes (beleértve az elektronikus azonosítás során keletkezett) adatokról,
- hostolt szerver elérése,
- a hatósági, az ügyészségi és a bírósági megkeresésekről, valamint az azok alapján teljesített adatszolgáltatásokról.
- a rendszerdokumentációk, szoftverek törzspéldányai és a biztonsági adathordozók.

5.2.3. Fontos („C" osztály)

- Nincs.

5.2.4. Nem kritikus („D” osztály)

5.3. Rendelkezésre állás szerinti osztályozás

5.3.1. Folytonos I. („A” osztály)

- záloghitel kezelő szoftver és a hozzá kapcsolódó adatbázis;
- a belépési és rendszerhasználati naplók adatai (audit trail, audit log, behatolási log a fizikai belépés ellenőrzés adatai, a biztonsági felügyelet naplója);
- internet szolgáltatás,
- tűzfal, switch, proxy,
- panaszkezelésre használt telefon.

5.3.2. Folytonos II. („B” osztály)

- felhasználói számítógépek, munkaállomások,
- hostolt szerver elérése,

5.3.3. Növelt redundancia („C” osztály)

- honlap (dinamikus),
- ügyfélforgalom biztosítására használt helyiségek.

5.3.4. Redundancia („D” osztály)

- honlap (statikus).

Az adatgazda az adatkezelések átláthatóságának biztosítása érdekében nem nyilvános adatvagyon nyilvántartást vezet, amely tartalmazza legalább:

a) a Társaság kezelésében lévő adatok felsorolását,

b) azt, hogy adott adat milyen informatikai rendszerben kerül kezelésre,

c) az adatok kezelésének és feldolgozásának fizikai helyszínét,

d) annak leírását, hogy az adatok esetleges továbbítása másik Adatkezelőhöz, illetve átadása adatfeldolgozók részére milyen módon történik, milyen biztonsági intézkedések mellett,

e) az adathoz milyen típusú munkavállalók vagy megbízottak férhetnek hozzá, ideértve az adatfeldolgozásra jogosult személyeket is.