Tanulmány a Biztonságos Kikötőre vonatkozó határozatban foglaltak alkalmazásáról II. rész.[1]

1.1.2Az alkalmazás anyagi hatálya

1.1.2.1. Az FTC (US Federal Trada Commission, az Egyesült Államok Szövetségi Kereskedelmi Bizottsága, SzKB) a DoT (US Department of Commerce), az Egyesült Államok Kereskedelmi Minisztériuma, EÁ KM) hatásköre.

A Biztonságos Kikötő (BK) rendszerben foglaltak alkalmazása jogszerűségének megítélése csak azokra a szektorokra és vagy adatfeldolgozó tevékenységekre vonatkozik, amelyek az SzKB vagy a KM hatáskörébe tartoznak.[2]

Kissé másképpen fogalmazva egy EÁ szervezet akkor alkalmazhatja a BK rendszerben foglalt rendelkezéseket, ha az adatok kezelése során igazolja, hogy alkalmazza az abban foglalt elveket, amely jogszerűségének megítélése az SzKB hatáskörébe tartozik, és az SzKB törvény 5. szakasza (amely tiltja a tisztességtelen és félrevezető gyakorlatokat) és az EÁ Kód 41712 bekezdése is tilt.

Félrevezető gyakorlatnak minősül, ha egy ésszerűen gondolkodó fogyasztóról anyagi értelemben valótlanságot állítanak vagy mulasztással vádolnak.[3] A Határozat III. bekezdése értelmében az SzKB-t széleskörű hatáskör illeti meg a fogyasztók adatainak gyűjtése és felhasználása jogszerűségének megítélése érdekében.[4] A Határozat III. függelékében foglalt rendelkezés értelmében, az SzKB-nek széleskörű hatáskörrel kell rendelkeznie ahhoz, hogy a fogyasztó adatai gyűjtésének és felhasználásának jogszerű voltát megítélje.[5] Következésképpen, ha egy amerikai szervezet önként igazolja, hogy adatkezelési gyakorlata megfelel a BK-ban foglalt elveknek, anélkül azonban, hogy a BK rendszert tiszteletben tartaná, úgy ennek megítélése az SzKB hatáskörébe tartozhat, mert ez „félrevezető gyakorlat" az SzKB jogszabályok előírásai szerint.

---

[1] Fordított: könyves Tóth Pál. Az eredeti letölthető:
http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf

[2] Lásd a Bizottság Határozata indokolásának 6. bekezdését.

[3] Egy gyakorlat akkor tisztességtelen, ha lényegesen sérti vagy sértheti a fogyasztó érdekeit, azt ésszerűen nem tudja elkerülni, s azt nem is ellensúlyozzák néki nyújtott előnyökkel és versenyelőnyökkel sem. Lásd: EÁ 15. Kód 45(n) bekezdését, és az SzKB elnökének, Mr. Robert Pitofskynak az Európai Bizottság XV. főigazgatósága igazgatójának Mr, John Moggnak 2000. július 14-én kelet levelét (lásd a Bizottság Határozatának V. függelékében foglaltakat is).

[4] Az SzKB elnöke a Pitofsykinak írt levelében egy Internet oldalra említ példát, ahol az a hamis állítás olvasható, hogy egy adatkezelő az adatokat állítólag a magánélet-védelmi politikájában foglaltaknak megfelelően, az önszabályozó útmutatások szerint kezeli, továbbá azt is, hogy az „SzKB-nek az az álláspontja, hogy az ilyen adatkezelés különös kihívást jelent a példátlan magánélet-védelmi gyakorlat számára, mert az veszélyezteti a gyermekek adatait vagy a felettébb érzékeny, például pénzügyi vagy egészségügyi információt is. Lásd továbbá a 6. gyakran feltett kérdést, mely szerint a közvélemény félrevezetésének minősül az az állítás, hogy egy szervezet az adatok kezelése során alkalmazza a BK-ban foglalt elveket, holott ezt valójában nem teszi meg, ám ennek megítélése az SzKB vagy más illetékes hatóság hatáskörébe tartozik, éspedig a Hamis Állításokról szóló törvény értelmében (EÁ Kód 18. fejezet, 1001. §).

[5] Az SzKB elnökének, Pitoskynak a levele egy Internet oldalra említ példát, amelyen az a hamis állítás olvasható, hogy egy állítólagos magánélet-védelmi politika vagy egy önszabályozó útmutatás megfelel a vonatkozó jogszabályok előírásainak, továbbá azt is állítja, éspedig hamisan, hogy az „SzKB álláspontja szerint a példátlan magánélet-védelmi gyakorlatok a Határozat 5. fejezete értelmében tisztességtelenek minősülnek, mert gyermekek személyes adatait kezelik vagy felettébb érzékeny adatokat, például pénzügyi és egészségügyi adatokat kezelnek." A 6. gyakran feltett kérdés szerint is „ha egy szervezet hamisan azt állítja vagy a közvéleményt bármi módon félrevezeti, hogy egy szervezet az adatokat a BK-ban foglalt elvekkel összhangban kezeli, úgy e kérdések megítélése az SzKB vagy más illetékes kormányzati testület hatáskörébe tartozik. A KM vagy megbízottja rendelkezéseinek megsértését a Hamis Állításokról szóló törvény előírásai szerint kell megítélni. (ÁE Kód 18. szakasz 1001. §.)

Néhány különbséget azonban hangsúlyozni kell.
Először is a bíróságok mindeddig nem erősítették meg, hogy az SzKB széleskörű hatáskörébe tartozik a magánélet-védelme jogszerű voltának megítélése.[6] Ámbár néhány eset kétségtelenül félrevezető gyakorlatnak minősíthető[7], egyéb esetek egy szürke zónába tartozhatnak, s az adatkezelőt valamint az adatalanyt bizonytalanságban hagyják. Az AE Kód 15. fejezete 45(n) bekezdése szerint egy gyakorlatot akkor kell „tisztességtelen"-nek tekinteni, ha súlyos hátrányokat okoz, vagy esetleg okozhat a fogyasztóknak, s azt ésszerűen nem tudják elkerülni, és azokat nem ellensúlyozzák a néki nyújtott előnyök vagy versenyelőnyök sem. A SzKB ellenőrzési jogosultsága csak marginális, jóllehet lehetővé teszi egy félrevezető kereskedelmi gyakorlat ellensúlyozását az adatalanynak nyújtott kereskedelmi előnyökkel. Ámbár az adatok feldolgozásának jogszerűségét esetről esetre kell megítélni, az SzKB az Európai Bizottságnak küldött levelében hangsúlyozta, hogy „ha egy vállalkozás adatkezelési gyakorlata nem igazodik a magánélet-védelmi politikájában foglalt elvekhez, úgy az valószínűleg 'félrevezető' gyakorlatnak minősül."[8]

Másodszor is az SzKB hatásköre csak a tisztességtelen vagy a félrevezető cselekmények vagy gyakorlatok megítélését öleli fel, vagy azokat a gyakorlatokat, amelyeket a „kereskedelemben folytatnak vagy befolyásolják a kereskedelmet". Ha vállalkozások gyűjtenek és dolgoznak fel személyes adatokat javak értékesítésének és szolgáltatások nyújtásának támogatására, úgy ez feltehetően kielégíti a „kereskedelem" igényeit.[9] Mindazonáltal meglehetősen kétséges az SzKB Illetékessége a BK séma tekintetében.[10] Az SzKB-nek például, elvileg, nincs hatásköre arra, hogy a nem kereskedelmi célra gyűjtött személyes információ gyűjtésének és feldolgozásának a jogszerűségét megítélje.[11] A Határozat III. függelékében foglaltak szerint inkább a gyűjtött adatok céljának kereskedelmi jellegét kell figyelembe venni, mint az adatkezelő kereskedelmi természetét.

Az alkalmazottakkal kapcsolatos személyes adatok vagy kutatási tevékenységek célját szolgáló feldolgozása (pl. személyes információ felhasználása kábítószerek kifejlesztésére vagy tesztelésére) jogszerűségének megítélése nem tartozik az SzKB hatáskörébe, és rendszerint a BK-éba sem. A gyakran feltett kérdések mindazonáltal különleges rendelkezéseket tartalmaznak az emberi erőforrásokkal kapcsolatos adatoknak az EÁ-ba irányuló továbbítását illetően, éspedig az adatok kutatási és/vagy egyéb célt szolgáló felhasználását illetően. A 29. cikk szerint Munkacsoport

---

[6] Lásd J.R. Reidenberg, "Privacy Wrongs in Search of Remedies," (Magánélet-védelmi sérelmek és orvoslásuk) cÍmű, a *Hastings Law Journal* 54. évfolyamában, 2003-ban, a 877-898. oldalon megjelent cikkét, különösen, ami a cikk 888. oldalán olvasható. („Minthogy minden olyan félrevezető gyakorlat, melynek jogszerű volta megítélése az SzKB hatáskörébe tartozik, méghozzá anélkül, hogy bármely bíróság döntött már volna róla, a törvényes szabályok bizonytalanok maradnak").

[7] Lásd pl. a Geocities and ReverseAuction.com eseteket (hivatkozva, *inter alia*, a Bizottság Határozatában). Ezeket az eseteket, mert nem tartoznak a bíróság hatáskörébe, az SzKB már rendezte.

[8] Lásd ugyancsak a Határozat III. függelékében foglaltakat.

[9] Lásd az SzKB elnökének, Ptofskynak a levelét.

[10] Lásd általában J.R. Reidengerg "Privacy Wrongs in Search of Remedies," (A magánélet-védelmi jogok sérelmei és orvoslásuk) című, és "ECommerce and Trans-Atlantic Privacy" „E-kereskedelem és a magánélet védelme a transzatlanti államokban) című cikkét, amely a *Houston Law Review* folyórat 28. évfolyamában jelent meg, 717-749. oldal, valamint Y. Poullet, "The Safe Harbour Principles – An adequate protection?" (A Biztonságos Kikötő elvei – megfelelő védelem?) című, az IFCLA által szervezett Nemzetközi Kollokviumon tartott előadását, Párizs, 2000. június 15-16. Letölthető: http://www.droit.fundp.ac.be/textes/safeharbor.pdf. (Felkeresve: 2004. február 28.).

[11] Lásd a határozat III. függelékében foglaltakat, és az SzKB elnökének a levelét, amelyben példát említ egy „chat room"-ra (csevegő szobára), melyet nem kereskedelmi jogi személyek működtetnek, hanem pl. szeretetszolgálatok.

megerősítette, hogy a személyes adatok efféle célokat szolgáló feldolgozása jogszerűségének megítélésének módját a BK nem tartalmazza.[12] Az SzKB-re vonatkozó jogszabályai kizárják az SzKB illetékességét a következő esetekben: (1) pénzügyi intézmények, ideértve a bankokat, hitel- és kölcsön egyesületüzemeltetők. eket is; (2) távközlési szolgáltatók és államok közötti közös szállítók; (3) légi szállítók; és csomagolók és raktár működtetők.

Ha a személyes adatok feldolgozását olyan szervezetek végzik, amelyek jogszerű voltának megítélése a KM hatáskörébe tartozik, ugyancsak igazolhatják, hogy működésük során alkalmazkodnak a BK-ban rögzített elvekhez. A KM, az EÁ Kód 49. szakasza 41712 bekezdésében foglaltak alapján, ami tiltja, hogy egy szállító „tisztességtelen vagy félrevezető" gyakorlatot folytasson, valamint tisztességtelen versenymódszereket alkalmazzon légi szállítmányok eladásakor, ami a fogyasztónak kárt okoz vagy okozhat. Az utasok védett információjának megsértése *per se* sérti az ebben a fejezetben meghatározott rendelkezéseket, kivéve, ha a szervezet nyilvánosan sértette meg az elveket.[13]

1.1.2.2 „Személyes adatok" továbbítása

A „személyes adatok" vagy „személyes információ" továbbítása csak akkor jogszerű, ha arra a BK-ban foglaltaknak megfelelően kerül sor, az adatoknak e kategóriái ugyanis meglehetősen bizonytalanul vannak meghatározva, úgy, mint „azonosítható vagy azonosított személy adatai, melyeket, ha az adatokat egy EÁ szervezetnek az EU-ból továbbítják, az Irányelv meghatározásaival összhangban kell továbbítani, majd bármilyen formában rögzíteni.[14] Ezek a meghatározások némi hasonlóságot mutatnak a 95/46/EK 2(a) bekezdésében foglalt, a „személyes adatok" meghatározásaival, ugyanis ezek a meghatározások bármely közvetlenül vagy közvetve azonosítható természetes személyre vonatkoznak, különösen, ha a személyt személyazonosító számával vagy másképp, fizikai, fiziológiai, mentális, anyagi helyzetére jellemző, kulturális vagy szociális adatai felhasználásával azonosítják.[15]

Azt az információt, mely viszonylag „anonim", egy közvetítő viszonylag könnyen „visszaazonosíthat" („kódolhatja" vagy „pszeudo-aninimizálhatja" az adatokat) az Irányelv rendelkezéseinek megfelelően kell kezelni, még akkor is, ha a BK-ban foglalt elvek ilyen információ kezelésére nem alkalmazhatók. Az „munkavállalókkal kapcsolatos adatok" esetében a 9. gyakran feltett kérdésben foglaltak

[12] A 29. cikk szerinti Adatvédelmi Munkacsoport vélemény szerint, az adatoknak ezeket a kategóriáinak továbbítását a BK-ban foglalt rendelkezések értelmében kifejezett meg kell tiltani. Lásd: *Opinion 7/99 on the Level of Data Protection provided by the 'Safe Harbor' Principles as published together with the Frequently Asked Questions (FAQs) and other related documents* (Vélemény a 'Biztonságos Kiköt' elveinek, valamint a gyakran feltett kérdésekben meghatározott elveinek megfelelő adatvédelem szintjéről. WP 27, 1999. november 15-16., 4-5. oldal. EÁ KM 1999. december 3.

[13] Lásd Mr. Samuel Podbereskynek a Légiforgalmi szabályok alkalmazását kikényszerítő és megsértésük esetén az eljárást lefolytató szervezet főtanácsadójának, Mr. John Mogg-nak, az Európai Bizottság XV. főosztálya igazgatójának küldött levelében foglaltakat. (Lásd továbbá: a Bizottság Határozata VI. függelékében foglaltakat is).

[14] Lásd a Bizottság Határozata I. függelékében foglaltakat.

[15] Lásd az Irányelv indoklásnak 26. bekezdését, amely úgy szól, hogy ha egy személy adatok felhasználásával azonosítható, akkor az adatkezelőnek vagy bármely más azonosítása érdekében. Ha egy egészségügyi program keretében például egy orvos vagy bárki más az egészségügyi adatok személyi azonosítóit egy véletlen számmal, amit egy számítógép rendel hozzá, helyettesítve megküldi egy gyógyszerészeti vállalkozásnak, az Irányelv rendelkezéseit kell alkalmazni, mert az információ szolgáltatója, pl. az orvos, az adatokat adott beteghez rendelheti. a „személyes adatok" meghatározásáról folyó további vitás kérdésekkel kapcsolatosan, lásd L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Adatvédelmi jog: a vitás kérdések ésszerűsége, logikája és határai) című cikkét a „The Hague: Kluwer Law International folyóirat 2002. évi évfolyamában, 41–50, 210–215, 315–319. oldalon.: oldalon. Az „aggregált adatok"-ról lásd *inter alia* D.J. Solove "On aggregte data: Privacy and Power: Computer Databases and Metaphors for Information Privacy", (A magánélet védelme és a hatalom, a magánélet-védelemre vonatkozó információ metamorfózisa), *Stanford Law Review*, 2001. 53. kötet, 1393–1462. és különösen az 1434 és 1452. oldalt.

kifejezetten kizárják az alkalmazások köréből az „anonimizált” vagy „pszeudoanoniminált” adatokat, éspedig anélkül, hogy tisztáznák értelmezésüket. A 14. gyakran feltett kérdésben foglaltak értelmében a kutatási adatoknak a legfőbb nyomozó által való továbbítása az EU-ból az EÁ-ba nem jelent egy olyan továbbítást, aminek alkalmaznia kellene a BK-ban foglalt elveket. Az azonban nem világos, hogy egyéb kategóriájú adatok feldolgozása módjának nem kellene alkalmazkodnia a BK rendszerhez.

Kissé határozottabban merül fel azonban az a kérdés, hogy mit kell érteni „anonimizálált” és „pszeudoanonimizált” adatokon. Folytonosság van ugyanis a tisztán személyes és anonim adatok között, sok adatkategória e két szélsőség közé esik. H például az adatok továbbítója és fogadója kölcsönösen függenek egymástól, úgy valószínűtlen, hogy az adatok teljesen „anonimizáltak”, hacsak ezt egy bizalmi harmadik fel nem garantálja.
A védelem „megfelelő” szintje nem szükségképpen egyezik meg a személyes adatok meghatározásával, ami azonos az Irányelv meghatározásával. Csak egy szűkebb meghatározás jelenthet terhet az adatalany magánéletét és ezzel kapcsolatos szabadságait veszélyeztető elfogadhatatlan kockázatok problémáinak megoldásár nézve.

A BK szövege szerint az amerikai jogszabályokat kell alkalmazni a BK-ban foglalt elvekkel kapcsolatos kérdések értelmezésére és a BK szervezetek vonatkozó magánélet-védelmi politikája megfelelősége eldöntése esetében is, kivéve, ha e szervezetek kötelezettséget vállaltak arra, hogy együttműködnek az európai adatvédelmi hatóságokkal (pl. emberi erőforrásokkal kapcsolatos adatok továbbítása jogszerűségének eldöntése esetében). Következésképpen az efféle adattovábbítás értelmezése az SzKB vagy a KM (esetleg egy amerikai bíróság) által végül is meghatározó. Mindazonáltal a BK keret kifinomult ellenőrző és mérlegelő rendszert tartalmaz. Ha az amerikai hatóságok értelmezése erodálja a Bizottság megállapításait, úgy ez utóbbinak újra kell gondolnia az elveket a Határozat 3(4) pontjában foglaltak szerint. Az 5. gyakran feltett kérdéssel összhangban egy EÁ szervezet együttműködhet az európai adatvédelmi hatóságokkal, mely esetben ez utóbbi értelmezése lesz első sorban az uralkodó.

1.1.3 Az alkalmazás alanyi hatálya
A BK-ban foglalt elvekhez csak EÁ szervezeteknek kell alkalmazkodniuk, mert ezek az elvek a BK dokumentumban nincsenek meghatározva. A Bizottság a Határozatában a maga részéről jelzi, hogy a BK-ban foglalt elvek kiindulásképpen nem alkalmazhatók azokra a természetes/fizikai személyekre, akiknek az EU-ból személyes adatokat továbbítanak. Mindazonáltal ha egy természetes személynek van egy üzleti vállalkozása, és annak egyedüli vagy többedmagával a tulajdonosa adatokat továbbít, úgy az, mint jogi személy, igazolhatja az adattovábbítás jogszerűségét. Több esetben az SzKB hatáskört igényelt azon személyek adatai továbbítása jogszerű volta megítélése érdekében, amelyek megsértették az SzKB törvényben foglaltakat, és büntetést szabtak ki rájuk, vagy megegyeztek e személyekkel, és a megegyezésből adódó előnyökben is részesülhettek.

Az „EÁ szervezetet nem lehet egyszerűen a 95/46/EK irányelvben foglalt „adatkezelő”-ként értelmezni. Az „EÁ szervezet” nem értelmezhető egyszerűen a 95/46/EK Irányelvben meghatározott „adatkezelő”-ként, a BK-ban foglalt elvek ugyanis, mint korábban már jeleztük, nem utalnak az EÁ hatóságok értelmezésére (mely hatóságoknak az értelmezésre vonatkozó felhatalmazása korlátozott, de az adatok védelme megfelelő szintjét meghatározhatják).

A BK-ban foglalt elvek, mint fentebb már említettük, nem hivatkoznak az Irányelvre, legalábbis az „EÁ szervezet” meghatározását tekintve, mert az elveket általában az EÁ hatóságai értelmezik (mely hatóságoknak az értelmezésre vonatkozó felhatalmazása korlátozott, mindazonáltal az adatok védelmének megfelelő szentjét meghatározhatják.

Az „EÁ szervezet” meghatározására több feltevést tehetünk, éspedig:
(i) főosztály, amely a BK rendszer szerint különálló szervezet. Ha például a személyes adatokat egy EU-ban letelepedett vállalkozás kezeli, s azokat továbbítja egy főosztályának, úgy az az érvényes szabályok értelmében nem minősül továbbításnak, mert az információ, vitathatatlanul, ugyanazon szervezeten belül cirkulál. Az Irányelvben foglaltak szerint egy „adatkezelő” szervezet határozza meg az adatok kezelésének és feldolgozásának céljait, s eszközeit, mely kezelést és feldolgozást ténylegesen főosztályainak egyike hajt végre;
(ii) ha az adatokat a különböző, de egy csoporthoz tartozó vállalkozások egymás közt megosztják, a helyzet kevésbé lesz világos, mert ennek a jogi kritériumait a BK dokumentáció nem határozza meg, legalábbis azt, hogy e vállalkozások különböző „szervezetekhez” tartoznak. A vállalkozások mindazonáltal valószínűleg különböző „szervezeteket”, még ha az adatok feldolgozását nem is a csoport[16] központi menedzsmentje iránymutatásai szerint dolgozzák is fel;
(iii) egy szervezet a BK megegyezés szerint egy másik szervezet megbízásából végzi a feldolgozó műveleteket, melyet elkülönült jogi személynek kell tekinteni. és meg kell különböztetni az adott „szervezettől”. Így egy „feldolgozó” az Irányelv szerint „harmadik félnek” minősülhet, ha egy ügynök helyett vagy utasításai szerint végzi a szervezet feladatait.[17]

Tény, hogy egy vállalkozás, amely egy másik jogi személlyel szerződéses kapcsolatban van, nem zárja k, hogy ez utóbbi „harmadik félnek” minősüljön, mert ennek ellenkezője aláásná az elveket. Az elvek általános értelmezéséből következtetni ehet a „harmadik fél” fogalmára, ámbár az ne világos, mi tekinthető elkülönült jogi személynek.[18]

Minthogy az Irányelv funkcionális megközelítést követ (pl. az adatkezelőt, mint *de facto* hatalmat határozza meg, amely az adatok feldolgozása céljait és eszközeit rögzíti), a BK megegyezés, úgy tűnik, egy vállalkozásokra vonatozó jogszabályi megközelítést követ, ami a „jogi személyiséget” egy „EÁ szervezet” elsődleges kritériumának tekinti.

1.1.4 Előzetes következtetések

Az olyan kulcsfontosságú koncepciók, mint az „EÁ szervezet”, „személyes adatok”, „félrevezető gyakorlatok” nincsenek világosan meghatározva, és az SzKB is kétértelműen határozza meg egyes adattípusok továbbításának feltételeit. Egy megbízható adatvédelmi rezsim esetében azonban nem szükséges meghatározni a konceptuális átláthatóságot, az azonban javasolható, hogy e koncepciók biztosítsák, hogy a vállalkozások ne igazoljanak olyan adattovábbításokat, amelyek kívül esnek a BK hatályán. Az erre vonatozó útmutatást a 29. cikk szerinti adatvédelmi Munkacsoportnak az SzKB/KM-mel együttműködve kellene kidolgoznia.

[16] Az elvek szerint egy „szervezet” „különálló jogi személy”, és nincsen felhatalmazva arra, hogy a feldolgozási művelet specifikumait meghatározza, mert erre a 6. gyakran feltett kérésben foglaltakból lehet következtetni, miszerint „egy szervezet, mint elkülönült jogi személy, megszűnik, egy összeolvadás vagy tulajdonosváltozás következtében, s ezt a KM-nek (vagy megbízottjának) is előzetesen be kell jelenteni”.

[17] Egy „harmadik személy” *per se* az Irányelv szerint nem minősül „feldolgozónak”, kivéve, ha feladatait az adott szervezet helyett vagy utasításait követve végzi. A feldolgozásról nem szükséges tájékoztatást adni, és megválasztani a vonatkozó elveket, másrészről azonban a BK-ban foglaltak 1 & 2 végjegyzetében foglaltakhoz kell alkalmazkodnia.

[18] A „harmadik fél” meghatározása analóg lehet a 95/46/EK Irányelvben foglalt meghatározással (ámbár elméletileg némileg másképpen), az Irányelv 2. cikke ugyanis a „harmadik fél” fogalmát a lövetlezőképpen határozza meg: „bármely természetes vagy jogi személy, közhatalmi hatóság vagy bármely más testület, amely adatalany, adatkezelő, adatfeldolgozó és az a személy, aki vagy amely az adatkezelő vagy –feldolgozó felhatalmazott az adatok feldolgozására.”
