Konzultáció

2012.04.05.

A konzultáció programja

10:00-10:15	Megnyitó	/Zsigrai Béla/
10:15-11:00	Tűzvédelem	/Fazekas Péter/
	Vendégelőadó: Mészáros Gábor tű. őrnagy, hatósági osztályvezető Kecskeméti Katasztrófavédelmi Kirendeltség	
11:00-11:40	Adatvédelem	/Czégány Béla/
11:40-12:00	Takarékszövetkezeti honlapok biztonsága	/Sipos Péter /
12:00-12:20	Szünet (kávé, üdítő, sütemény)	
12:20-12:40	Munkavédelem	/ Zsigrainé Hegedűs Ildikó /
12:40-13:00	Fogyasztóvédelem	/ dr. Szegő Annamária /
13:00-13:30	Pénzmosás-megelőzés	/ dr. Bibok Imre /
13:30-14:00	Konzultáció, kérdések, egyedi esetek megvitatása az előadásokat követően.	

Tűzvédelem

Jogszabályváltozások

- változás: 30/1996. (XII.6.) BM rendelet a tűzvédelmi szabályzat készítéséről – új ponttal bővült
- új jogszabály: 28/2011. (IX. 6.) BM rendelet az Országos Tűzvédelmi Szabályzatról (a továbbiakban OTSZ; hatályos 2011.10.06-tól)
- hatályát vesztette: 9/2008. (II. 22.) ÖTM rendelet az Országos Tűzvédelmi Szabályzat kiadásáról
- új jogszabály: 259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról

Első fokú tűzvédelmi hatóság

259/2011. (XII. 7.) Korm. rendelet a tűzvédelmi hatósági feladatokat ellátó szervezetekről, a tűzvédelmi bírságról és a tűzvédelemmel foglalkozók kötelező élet- és balesetbiztosításáról

1. § (1) A Kormány első fokú tűzvédelmi hatóságként …
a katasztrófavédelmi kirendeltséget jelöli ki, amely

c) a létesítmény, az építmény, a helyiség vagy a szabadtér területén a tűzvédelmi létesítési és használati szabályok betartását ellenőrzi,

f) az üzemeltetést, a tevékenységet a tűzvédelmi követelmények érvényesítéséig megtilthatja, ha

fa) a helyiségben, az önálló rendeltetési egységben, az építményben, a szabadtéren a megengedett maximális befogadóképességet 15%-nál nagyobb mértékben meghaladják, vagy azt az arra kötelezettek a Tűzvédelmi Szabályzatban nem állapították meg, vagy a kiürítési feltételeket nem biztosítják,…

Maximális befogadóképesség

- 30/1996. (XII. 6.) BM rendelet a tűzvédelmi szabályzat készítéséről
- 3. § A Szabályzatnak tartalmaznia kell:

  i) a tevékenység helyszínét képező és 50 főnél nagyobb befogadóképességű helyiséget tartalmazó önálló rendeltetési egység vagy önálló rendeltetési egységen belüli, helyiségcsoport (építményrész) esetében a - kiürítési számítással vagy azzal egyenértékű módon igazolt - megengedett maximális befogadóképességet;

  j) az i) pont szerinti esetekben a megengedett maximális befogadóképességnek megfelelő helyiséghasználat módját és felelősét.

Menekülési útvonalak

- OTSZ 470. § (1) A kiürítésre számításba vett nyílászáró szerkezetek –kivéve a legfeljebb 50 fő tartózkodására szolgáló helyiségeket és az arra minősített nyílászárókat– csak a kiürítés irányába nyílhatnak.
- 473. § A kiürítés céljára 50 főnél több személy esetében íves karú lépcsőt számításba venni nem szabad.

- OTSZ 575.§ (4) A menekülési útvonal leszűkítése –a kiürítéshez szükséges átbocsátóképesség méretéig–, továbbá ott éghető anyag tárolása, burkolat elhelyezése a tűzvédelmi hatóság engedélyével történhet.
- (6) A kiürítésre és menekülésre számításba vett nyílászáró szerkezeteket – kivéve a legfeljebb 50 fő tartózkodására szolgáló helyiségeket és az arra minősített nyílászárókat –, míg a helyiségben tartózkodnak, lezárni nem szabad.

Tűzoltó készülék ellenőrzése

- OTSZ 13. § (1) A készenlétben tartó vagy képviselője a rendszeresen, legalább negyedévente ellenőrzi, hogy a tűzoltó készülék
  - a) az előírt telepítési helyen van,
  - b) rögzítése biztonságos,
  - c) látható,
  - d) magyar nyelvű használati utasítása a tűzoltó készülékkel szemben állva olvasható,
  - e) használata nem ütközik akadályba,
  - f) valamennyi nyomásmérő vagy jelző műszerének jelzése a működési zónában található,
  - g) hiánytalan szerelvényekkel ellátott,
  - h) fém vagy műanyag plombája, karbantartást igazoló címkéje sértetlen és ép,
  - i) zárópecsétje sértetlen,
  - j) felülvizsgálata esedékes-e, és
  - k) állapota kifogástalan, üzemszerű.
- (2) A vizsgálatot a karbantartó szervezet is végezheti.

Tűzvédelmi szabványossági felülvizsgálat, Villámvédelmi felülvizsgálat

- OTSZ 213.§ (2) A villamos berendezés használatbavételét követően, a berendezés üzemeltetője, ha jogszabály másként nem rendelkezik

b) a „C”, „D” és „E” tűzveszélyességi osztályba tartozó helyiségben, szabadtéren legalább hatévenként a villamos berendezés tűzvédelmi felülvizsgálatát elvégezteti, és a tapasztalt hiányosságokat a minősítő iratban meghatározott határnapig megszüntetteti, melynek tényét hitelt érdemlő módon igazolja.

(3) A tűzvédelmi felülvizsgálat szempontjából a naptári napot kell figyelembe venni.

- OTSZ 226.§ (2) A villámvédelmi berendezést – ha jogszabály másként nem rendelkezik …

  b) egyéb esetben legalább hatévenként, tűzvédelmi szempontból felül kell vizsgáltatni, és a tapasztalt hiányosságokat a minősítő iratban meghatározott határnapig meg kell szüntetni, melyek tényét hitelt érdemlő módon igazolni kell.

Beépített tűzjelző berendezés telepítése

- OTSZ 136. §

  Beépített tűzjelző/tűzoltó berendezést kell létesíteni a jogszabály 7. melléklet 1. táblázatában foglalt esetekben,

  (iroda rendeltetés, többszintes és 13,65m felett kialakított, ha a rendeltetés az 500m^2-t meghaladja)

  továbbá ahol azt a fennálló veszélyhelyzetre, az építmény nemzetbiztonsági, nemzetgazdasági, műemlékvédelmi vagy adatvédelmi jellegére, az építményben tartózkodók biztonságára, valamint a tűzoltóság vonulási távolságára tekintettel a tűzvédelmi hatóság előírja. Ezen előírást új *(a rendelet hatályba lépése után átadott)* létesítménynél, építménynél, valamint a meglévő (építési engedély köteles) átalakításakor kell alkalmazni.

Átjelzés a Tűzoltósági ügyeletre

- OTSZ 139. § (1) A beépített tűzjelző vagy tűzoltó berendezés tűzjelzését, az állandó felügyelet mellett, automatikus átjelzéssel kell továbbítani az elsődleges működési körzet szerinti tűzoltóságot riasztó hírközpontba (a továbbiakban: tűzoltósági ügyelet)

  …

- j) a 8000 m^2-nél nagyobb alapterületű, vagy három szintnél magasabb kereskedelmi építmény esetén.

- A (1) bekezdésben előírt tűzátjelzést csak akkor kell kiépíteni, ha a tűzoltósági ügyelet a vonatkozó műszaki követelménynek megfelelő módon képes azt fogadni.

	Tűzvédelmi szabálytalanság (kivonat)	Tűzvédelmi bírság legkisebb mértéke /Ft/	Tűzvédelmi bírság legnagyobb mértéke /Ft/
1.	Tűzvédelmi előírás megszegése, ha az tüzet idézett elő	100 000	1 000 000
2.	Tűzvédelmi szabály megszegése, ha az tüzet idézett elő és az oltási tevékenységben a tűzoltóság beavatkozása is szükséges	200 000	3 000 000
3.	Tűzvédelmi szabály megszegése, ha azzal közvetlen tűz vagy robbanásveszélyt idéztek elő	100 000	1 000 000
4.	Menekülésre számításba vett kijárat, vészkijárat leszűkítése, oly módon, hogy a kiürítéshez szükséges átbocsátóképesség nem biztosított	30 000 /kijárat	45 000 /kijárat
6.	Menekülésre számításba vett kijárat, vészkijárat lezárása, leszűkítése oly módon, hogy a menekülő számára az nem szüntethető meg azonnal	200 000 /kijárat	300 000 /kijárat
8.	Kiürítésre figyelembe vett közlekedőn, folyosón éghető anyagok, tárgyak elhelyezése a tűzvédelmi hatóság engedélye nélkül	60 000 /közlekedő	100 000 /közlekedő
9.	Az I. fokú tűzvédelmi hatósággal történt egyeztetés nélkül a kiürítésre figyelembe vett közlekedőn, folyosón éghető installációk, dekorációk, szőnyegek, falikárpitok, továbbá egyéb éghető anyagoknak az elhelyezéssel érintett fal- vagy a padló felületének 30%-ánál nagyobb mértékű részét borító elhelyezése *(a beépített építési termékek és biztonsági jelek kivételével)*	100 000	1 000 000
11	Jogszabály, vagy hatóság által előírt, a tűz- vagy füstszakasz határon beépített tűz- vagy füstgátló műszaki megoldás megszüntetése, eltávolítása, működésének akadályoztatása *(ide tartoznak a tűzmentes irattárak minősített tűzgátló ajtói is, melyeknek automatikusan be kell csukódniuk / behúzószerkezettel)*	60 000	200 000
16	Tűzoltó készülék készenlétben tartásának, karbantartásának:		
	– készenlétben tartás hiánya *(nincs készülék)*	50 000 /készülék	
	– karbantartás hiánya *(van, de a karbantartása nem történt meg, felülvizsgálat érvényessége lejárt)*	30 000 /készülék	

	Tűzvédelmi szabálytalanság (kivonat)	Tűzvédelmi bírság legkisebb mértéke /Ft/	Tűzvédelmi bírság legnagyobb mértéke /Ft/
	Jogszabály vagy hatóság által előírt beépített tűzjelző vagy tűzoltó berendezés készenlétben tartásának, karbantartásának, felülvizsgálatának hiánya, működésének akadályozása, *(ide tartozik a 28/2011. (IX. 6.) BM rendelet 8. számú mellékletében szereplő (tűzjelző központ üzemeltetési) napló vezetésének elmulasztása vagy hiányossága)* ha a védett tér		
17	a) legfeljebb 100 m^2 alapterületű:	100 000 /rendszer	400 000 /rendszer
	b) 101–500 m^2 alapterületű:	200 000 /rendszer	1 000 000 /rendszer
	c) 500 m^2 feletti alapterületű:	400 000 /rendszer	2 000 000 /rendszer
18	Tűzjelző vagy tűzoltó berendezés központjának jogszabály vagy hatóság által előírt állandó felügyelet, közvetlen tűzátjelzés hiánya *(a tűzjelző központ jelzései nem futnak be a diszpécserszolgálathoz, vagy a tűzoltósághoz, ill. az átjelzés szerződés szerint nem biztosított)*	150 000 /rendszer	1 500 000 /rendszer
27	Ha a munkáltató az új munkavállalók tűzvédelmi oktatásáról, illetve a tűzvédelmi szabályzat megismertetéséről a munkába lépéskor – igazolt módon – nem gondoskodott, és a munkavállaló belépése óta több mint 15 nap eltelt	100 000 /munkavállaló	
28	Ha a munkáltató a munkavállalók ismétlődő vagy a tűzvédelmi hatóság által előírt soron kívüli tűzvédelmi oktatásáról, illetve a tűzvédelmi szabályzat megismertetéséről a jogszabályban vagy a tűzvédelmi szabályzatában, a soron kívüli oktatást előíró határozatban rögzített határidőre – igazolt módon – nem gondoskodott és a határidő óta több mint 15 nap eltelt	100 000 /munkavállaló	
33	A kötelező időszakos villamos vagy villámvédelmi felülvizsgálat hiánya *(a villamos berendezések tűzvédelmi szabványossági felülvizsgálatát és (ha van villámhárító) a villámvédelmi mérést és felülvizsgálatot egyaránt a 28/2011. (IX. 6.) BM rendelet (OTSZ) előírásai szerint, 6 évente kell végeztetni – naptári napot kell figyelembe venni)*	100 000 /rendszer	1 000 000 /rendszer
34	A fenti minősítő iratban feltárt – tűzveszélyes vagy soron kívüli, javítandó jelzéssel ellátott – hibák igazolt megszüntetésének hiánya	50 000 /rendszer	300 000 /rendszer
40	Egyéb tűzvédelmi jogszabályban vagy a tűzvédelmi szabályzatokban foglalt előírások, továbbá a tűzvédelmi szabványok előírásainak megszegése esetén	20 000	60 000

Köszönöm figyelmüket!

Adatvédelmi nyilvántartásba való bejelentkezés szabályai, határidők

Törvényi háttér

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- **Nemzeti Adatvédelmi és Információszabadság Hatóság** *(autonóm államigazgatási szerv - független csak a törvénynek van alárendelve, nem utasítható)*

  Feladatai:
  - Vizsgálatokat, hatósági eljárásokat folytat le
  - Adatvédelmi nyilvántartást vezet
  - Hatósági jogkörökkel rendelkezik
    - Törvényjavaslatok, ajánlások készítése
    - „Aggály” helyett bírság

Az adatbejelentés szabályai

- 2012. január 1. után, az adatvédelmi nyilvántartásba vételért igazgatási szolgáltatási díjat kell fizetni.

  (külön rendelet szerint, amely azonban még nem jelent meg)

- A 2012. január 1-jét megelőzően megkezdett, de az adatvédelmi nyilvántartásba be nem jelentett adatkezelést 2012. június 30-át követően nem folytathatja a Takarékszövetkezet ha azt 2012. június 30-ig nem jelenti be.

- A formanyomtatvány letölthető a Hatóság honlapjáról: www.naih.hu/bejelentkezes.html

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG
1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Tel: +36 (1) 391-1400 Fax: +36 (1) 391-1410 e-mail: ugyfelszolgalat@naih.hu

Tájékoztató az adatvédelmi nyilvántartásba érkezett bejelentések feldolgozásáról

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) értelmében 2012. január 1-jétől a Nemzeti Adatvédelmi és Információszabadság Hatóság (Hatóság) vezeti az adatvédelmi nyilvántartást, továbbá eljár az adatvédelmi biztoshoz 2012. január 1-je előtt érkezett, folyamatban lévő bejelentések tekintetében is.

A Hatóság a 2011. december 23-át megelőző három évre visszamenőleg közel 3000 olyan folyamatban lévő bejelentési ügyet vett át, amelyek adatvédelmi nyilvántartásba vételét az adatvédelmi biztos elmulasztotta, és bár törvényi kötelezettsége lett volna, az adatkezelőknek adatvédelmi nyilvántartási számot nem bocsátott ki.

2011. december 23-át követően pedig hozzávetőlegesen 2000 beadvány érkezett, amelyek már a Hatóságnál kerülnek iktatásra. Ebből adódóan a Hatóság hatalmas ügyhátralékkal indul.

A jelentős felhalmozódott ügyhátralék mellett a Hatóság munkáját nehezíti az is, hogy az Adatvédelmi Biztos Irodájából átvett informatikai rendszer elavult, ennek fejlesztése is a Hatóságra váró feladat.

A Hatóság ezzel a súlyos örökséggel kezdte meg munkáját, amely során azonban figyelembe kell vennie azt is, hogy az Infotv. fontos változásokat vezetett be az adatvédelmi nyilvántartás szabályozásában.

Az Infotv. – a korábban hatályos adatvédelmi törvénytől eltérően – bevezette, hogy 2012. január 1-jét követően a pénzügyi szervezetek, a közüzemi szolgáltatók, illetve az elektronikus hírközlési szolgáltatók kötelesek a Hatóságnál kezdeményezni ügyfeleik személyes adataival folytatott adatkezelések nyilvántartásba vételét.

Az Infotv. 68. § (1) bekezdése kimondja, hogy a Hatóság az adatkezelést a kérelem megérkezésétől számított nyolc napon belül nyilvántartásba veszi, amennyiben az megfelel a törvényben meghatározott tartalmi kritériumoknak. Az átvett és az újonnan érkezett adatkezelések nyilvántartásba vétele megkezdődött, azonban a jelentős ügyhátralék miatt a törvényi határidő betartása nehézségekbe ütközik. Emiatt a Hatóság az adatkezelők szíves türelmét kéri.

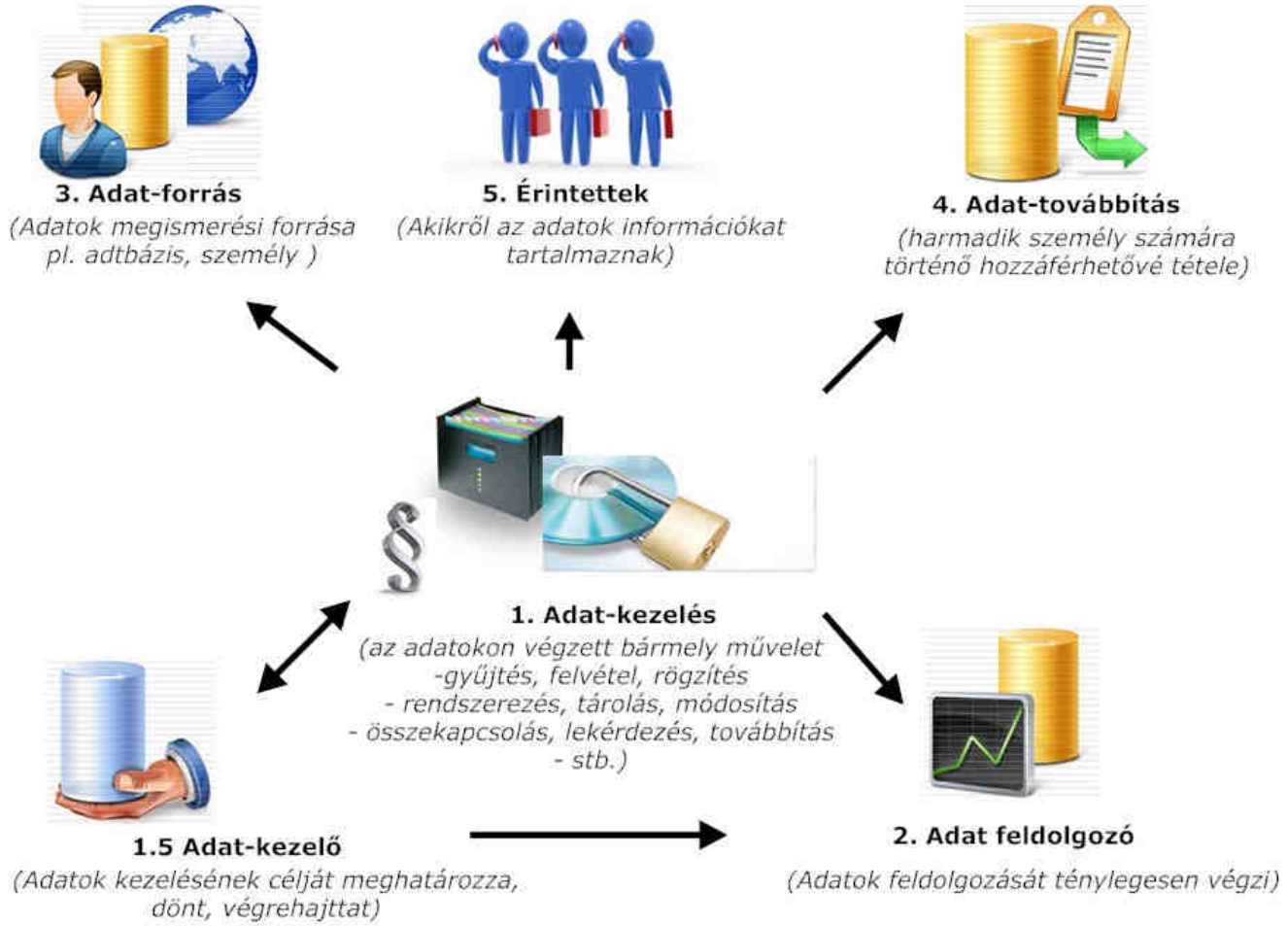
A Hatóság felhívja az adatkezelők figyelmét arra, hogy az Infotv. 68. § (2) bekezdése értelmében az adatkezelést a kérelmükben foglaltak szerint megkezdhetik, amennyiben a Hatóság a nyilvántartásba vétel iránti kérelmet határidőben nem bírálja el. Az adatkezelőknek azonban ez esetben is tekintettel kell lenniük az Infotv.-ben foglalt egyéb kötelezettségeikre, különösen az adatkezelés céljára, jogalapjára és az adatbiztonságra vonatkozó szabályokra.

A Hatóság tájékoztatja az adatkezelőket, hogy az adatvédelmi nyilvántartásba vételért igazgatási szolgáltatási díjat majd az azt meghatározó miniszteri rendelet hatályba lépése után beérkezett bejelentésekért kell megfizetni.

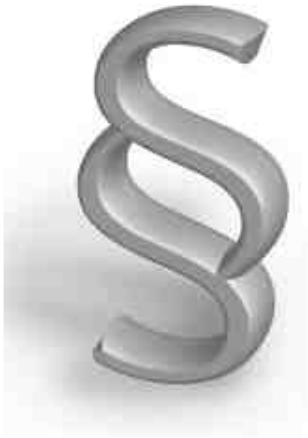
Budapest, 2012. január 19.

Dr. Péterfalvi Attila s.k
a NAIH elnöke

Az adatvédelmi nyilvántartás adatbázis szerkezete



Alapvető adatkezelési normatívák



- Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető.
- Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósításához elengedhetetlen a cél elérése érdekében.
- Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
- Személyes adat csak akkor kezelhető, ha ahhoz az érintett hozzájárult *(hozzájáruláson alapuló adatkezelés)* vagy azt törvény, vagy önkormányzati rendelet elrendeli (*kötelező adatkezelés*).

Alapvető adatkezelési normatívák

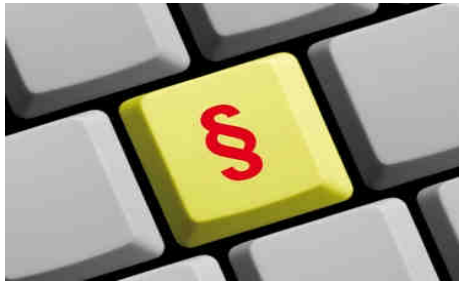
- Személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költségekkel járna, és a személyes adat:
  - Az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges
  - Az adatkezelő vagy harmadik személy jogos érdekének érvényesítése miatt szükséges, és az az adatok védelméhez fűződő jog korlátozásával arányban áll.
- A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható.

Alapvető adatkezelési normatívák

- **Ha az adatkezelés célja az adatkezelővel írásban kötött szerződés végrehajtása, a szerződésnek tartalmaznia kell:**
  - A kezelendő adatok meghatározását
  - Az adatkezelés időtartamát
  - A felhasználás célját
  - Az adatok továbbításának tényét, címzettjeit
  - Adatfeldolgozó igénybevételének tényét
  - Jogorvoslati lehetőségeket, érintett jogait, kötelezettségeit
  - A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett hozzájárul a szerződésben foglalt módon az adatai kezeléséhez.

PSZÁF 7/2011. számú módszertani útmutatója az internetbanki szolgáltatások biztonságáról

Célja, hatóköre



- **A Takarékszövetkezet felelős az internetbanki szolgáltatása keretében folytatott tranzakciók és tárolt adatok biztonságáért.**
- Nemzetközi „*legjobb gyakorlat*” alapján javasolható ajánlásokat és követendő gyakorlatokat tartalmaz
- Az ajánlás a hatályos jogszabályokkal együttesen támogatja a biztonságos informatikai üzemeltetést
- Az ***„útmutató ajánlásainak követése nem jogszabályon alapuló kötelezettség, de a Felügyelet tapasztalatai és véleménye szerint azok figyelembevétele nélkülözhetetlen az internetes banki szolgáltatások biztonságos üzemeltetéséhez”*** (részlet az ajánlásból).
- Hatóköre kiterjed a Takarékszövetkezet internetbanki rendszerének eszközeire, hálózati környezetére, és az üzemeltetésre.

Felsővezetői felügyelet

- **A Takarékszövetkezetnek azonosítania kell az internetbank használatával szükségszerűen együtt járó kockázatokat**

Ennek érdekében a Takarékszövetkezet

- legalább évente átvizsgálja az internetbanki rendszerét, feltárja a működésben rejlő informatikai kockázatokat
- rendelkezik az ügyfél azonosítási valamint a tranzakciós adatok átvitelénél alkalmazott védelmi és hitelesítési eljárások leírásával (auditálható).
- csalásfelderítő rendszert működtet (robotok, pókok)
- rendelkezik előre nem tervezett rendszerkiesések kezelésére vonatkozó üzletmenet folytonossági tervvel (felelősök megjelölésével). Ezeket időszakosan teszteli.

Ügyféloldali biztonság

- **Az internetbanki folyamatban az ügyfél magatartása, végfelhasználói eszközei jelentős kockázatot hordoznak.**

- Oktatás, tájékoztatás, figyelemfelhívás
  - Személyi azonosítók használata, biztonságos kezelése (több szintű)
  - Vírusvédelmi és kémprogram figyelő alkalmazások jelentősége
  - Adathalász módszerek szűrése (email)
  - Azonosító adatok elvesztése, visszaélési kísérletek észlelése esetén követendő eljárások
  - Nyilvános hálózatokon, nem saját gépen történő internetbank használat veszélyei
- Biztonsági bejelentések 24 órás fogadása, gyors szakszerű biztonsági intézkedések

Naplózás, jelszavak

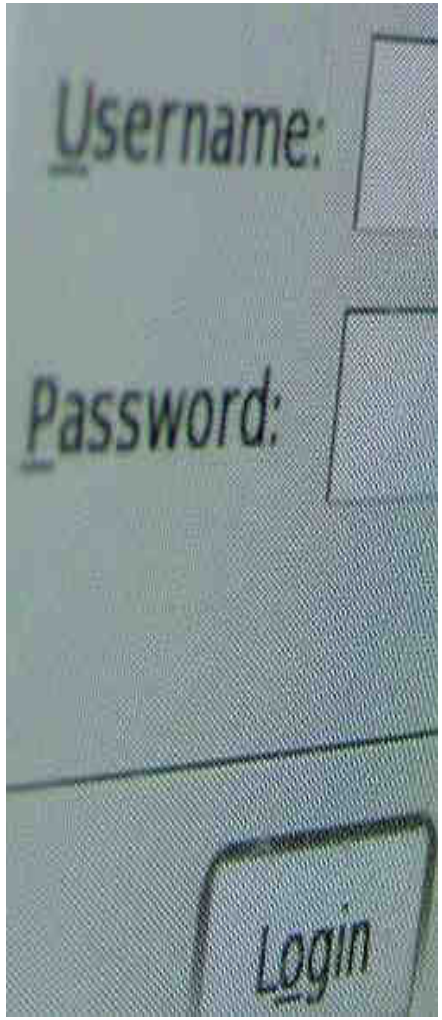
- Üzemeltetőknek és fejlesztőknek csak a műszakilag szükséges legalacsonyabb szintű hozzáférés biztosítása
- Rendszer zártsága, csak az internet banki alkalmazáson keresztül lehessen hozzáférni az adatbázishoz
- Külső partnerek által végzett tevékenységekről részletes naplók készüljenek
- Kapcsolatok csak a szükséges időintervallumig érvényesek (automata bontás, letiltás)
- Felhasználói jelszavak hálózati átvitele és tárolása rejtjelezetten történik
  - 90 napig érvényes jelszó (kikényszerítve)
  - Jelszó legalább 7 karakter, kis, nagybetű, szám
  - Választható jelszavak a legutolsó 4 jelszótól különbözőek
  - 5 sikertelen belépési kísérlet után a felhasználó tiltásra kerül
- Munkamenetek folyamatos naplózása, a napló védelme az illetéktelen módosítások ellen (forma, adathordozó)
- Hiteles időszerverre csatlakozik minden komponens

Üzemeltetési biztonság

- **A Felügyelet az internetbanki rendszerek üzemeltetésében a magas informatikai biztonsági szint megvalósítását javasolja**

- Folyamatos védelem tűzfal konfiguráció. A tűzfalak alapból mindent tiltanak *(deny all)*.
- Tűzfalszabályok felülvizsgálata 6 havonta
- Minden üzembe helyezett eszköz alapértelmezett biztonsági paramétereinek megváltoztatása
- Biztonsági házirendek a beállításokhoz, és azok folyamatos kontrollja
- Gyártói javító csomagok maximum 60 napon belüli telepítése
- Naprakész vírusvédelmi rendszer üzemel (riasztások)
- Tartalék eszközök, és megoldások amelyekkel az elvárt helyreállítási időn belül az internetbank működése helyreállítható
- Helyreállítási idők gyakorlati tesztelése

Ügyfél azonosítása



- **Az internetbanki alkalmazások meghatározó pontja az ügyfél személyazonosságának távoli ellenőrzése**
  - Egyfaktoros azonosítás (felhasználónév, jelszó)
    - Nem nyújt megfelelő biztonságot
    - Korlátozásokat kell alkalmazni
  - Többfaktoros azonosítás
    - Internetbanki kapcsolattól elkülönülő csatorna használata
    - Kiegészül egy nem statikus résszel
    - Véletlenszerű és/vagy időkorlátos adat, token által generált időkorlátos véletlenszerű számsorozat

Kiegészítő védelmi intézkedések

- Sikeres és/vagy sikertelen bejelentkezésről SMS/Email üzenet a felhasználónak
- Virtuális billentyűzet használata az azonosító adatok bevitelére
- Ismételt sikertelen bejelentkezési kísérleteket követően „grafikus kód” alkalmazása

Ügyfél-azonosítás ajánlások

Az alkalmazott azonosítási módszer legyen azonos az általa végezhető internetbanki műveletek kockázataival

- Biztonságos kommunikációs csatorna kiépítése a teljes munkamenetben (SSL/TLS, IPSEC)
- Statikus jelszavak esetén (legalább) az alábbi védelmi intézkedések
  - Sikertelen belépési kísérletek után automatikus kitiltás (időintervallum)
  - Sikertelen belépési kísérletekről az ügyfél tájékoztatása (SMS, Email, következő belépési képernyő)
- A független csatornán eljuttatott jelszó max. 10 percig érvényes
- SMS tájékoztatás küldése (egyenleg, azonosító adatok változása stb.)

Elektronikus tranzakció megőrzése

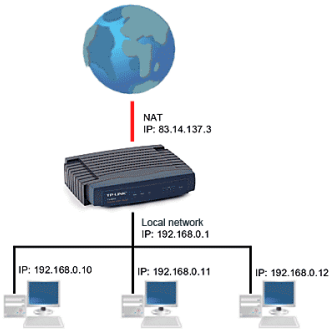
A Takarékszövetkezet hitelesítse az elektronikus tranzakciós üzeneteit, és gondoskodjon azok biztonságos őrzéséről

- Az internetbanki tranzakciós üzeneteket aláírással és időbélyeggel kell ellátni
- Minősített időbélyegzés használata, vagy időbélyegzés-szolgáltató alkalmazása
- Megőrzési idő min. 5 év.
- A hitelesített tranzakciókról legalább naponta mentés készül

2011. évi felügyeleti ellenőrzések tapasztalatai

Ellenőrzések főbb területei

- Infrastruktúra
  - Távadat-átvitel biztonsága
    - Tűzfalak, routerek beállításai, azok kontrollja
      - Rendszergazdai beállítások, felülvizsgálatok
  - Belső visszaélési lehetőségek
    - Belső ellenőri vizsgálatok
      - Be-kilépési idők (intervallum, munkaidő összevetése, szabadságok)
      - Munkavállalókhoz rendelt jogosultságok
      - Ugrókódok lekérdezésének gyakorisága, alapja, dokumentálása
      - Script-ek futtatása, dokumentálása
      - Ügyviteli szoftver naplóinak ellenőrzése (mentések)
      - Jelszóváltoztatás menetének ellenőrzése, dokumentálása
      - Technikai felhasználók nyilvántartása



Adatbázis hozzáférések

- Felhasználók rendszerbe léptetése
  - PC szintű belépés
  - Domain bejelentkezés
- Adatbázis módosítások naplózása
- A naplók manipulálhatósága
- Adatbázis közvetlen hozzáférések
  - adatbázis szinten
  - fájl szinten *(az adatbázisfájlokat csak a rendszergazda érje el)*
  - módosítások mentése, keretprogramba töltése

Köszönöm figyelmüket!

Takarékszövetkezeti honlapok biztonsága

Az előadás vázlata

- esetleges feltörések és ezek következményei
- védekezés lehetséges módszerei
- szolgáltató, üzemeltető kiválasztásának szempontjai

Honlapok sebezhetőségei

Amiről szó lesz:

- Mit értünk webes sebezhetőségek alatt?
- „Cyber Crime” napjainkban, valódi veszélyt jelent vagy csak rémhír keltés?
- Presztízsbeli és adatbiztonsági kockázatok a Takarékszövetkezet esetében,
- Adathalászat avagy „phishing”.
- Védekezési lehetőségek, megelőző lépések

Sebezhetőségek

- Webes sebezhetőségek: honlapok biztonsági kockázatai, hacker-ek támadásai
- Szerver felőli támadások, szerverkörnyezet, hálózat hiányosságai, hibái, tűzfal nem megfelelő konfigurációja
- Böngésző oldali támadások, fájlfeltöltés, hozzászólások, bejelentkezések.
- „szép” honlap ≠ biztonságos honlap, a biztonsági réseket a honlapok „motorjában” kell keresni és nem a küllemében.
- A gyakori karbantartás, ellenőrzés sok esetben megakadályozhat egy sikeres támadást

Sebezhetőségek

- A weboldalak fejlesztői által meghagyott hiányosságok jelentik a legnagyobb veszélyt. (kivédhető, elkövető általában „Script-kiddie”)
- „0day vulnerability” vagy „zero-day attack” még nem ismert, új hiányosságok kihasználása. (nehezen védhető, elkövető általában tapasztalt „hacker”)
- SQL alapú támadás, amely a különböző űrlapmezőkön keresztüli betöréseket jelenti
- URI-ból, megpróbálja feltérképezni a honlap szerkezetét
- Nem biztonságos jelszavak
- Munkamenet kezelési hibák, munkamenet tárol egyes információkat a látogatókról, melyeket a felhasználó gépén a sütikkel (cookie) azonosítanak

Sebezhetőségek

- Felhasználói bejelentkezések és regisztrációk engedélyezése a takarékszövetkezeti honlapon? Szükséges-e? Tölthetnek-e fel fájlt, küldhetnek-e onnan emailt, üzenetet?
- A nem megfelelően kezelt fájlfeltöltések nagy kockázatot jelenthetnek, ugyanis a fájlok akár kártékony kódot is tartalmazhatnak.
- Az egyik feltöltött fájlokba, akár képekbe, pdf állományokba is rejthetnek javascript kódokat amik különböző problémákat okozhatnak.
- Túlterheléses támadások a webes felületen, amelyek lassulást vagy szolgáltatás leállást okozhatnak.
- Tényleges betörések, melyek során az adatok biztonsága sérülhet.

Cyber bűnözés napjainkban

- Az IT hírek között megszaporodtak a cyber bűnözésről szóló cikkek.
- Valódi a veszély? Kik az elkövetők?
- LulzSec, Anonymous, TeaMp0isoN, Masters of Deception, stb..
- Nemzetek közti hacker támadások.
- Napjainkban a számítástechnikai információ áramlás hangsúlyosabb a hagyományos formátumoknál, így az azok ellen intézett támadások is gyakoribbá váltak.
- Elérendő célok a hackerek előtt:
  - információ szerzés
  - károkozás
  - politikai befolyás
  - figyelem felhívás
  - „terrorcselekmény”

Cyber bűnözés napjainkban

- A hackerek kategorizálása:
  - BlackHAT hacker:
    - károkozás, betörés, információ szerzés, Zero-day attack
    - Szabadúszók, vagy megbízatásra dolgoznak
    - Nagytudású szakember
  - WhiteHAT hacker:
    - Sebezhetőségek felderítése és kijavítása
    - Biztonságtechnikai cégek jól megfizetett nagytudású szakemberei
    - „Etical Hacker”, penetration tester
  - „GrayHAT” hacker (a fenti kettő kombinációja)
    - Szabadúszó, kedvtelésből tör be rendszerekbe, de kárt nem tesz, adatokat nem tulajdonít el

Cyber bűnözés napjainkban

- Script kiddie:
  - Mások által megírt kódokat felhasználva, már rég ismert hiányosságokat kihasználva hajt végre általában nem nagy jelentőségű betöréseket, gyakran kárt okoz.

- Hacker csoportok:ezen személyek gyűjtő csoportja akik összehangolt támadásokat hajtanak végre.

- Utóbbi időkben a Script kiddie csoportok nagy nyilvánosság előtt is nyíltan, sok és nagy média visszhangot jelentő ám nem túl jelentős „támadásokat” hajtanak végre.

- Valós veszély, gyakorlatilag egy weboldal sem lehet teljesen biztonságban.

Kockázatok a Takarékszövetkezetre nézve

- Például: Dühös ügyfél aki sérelmeit interneten teszi közzé, amire felfigyel egy csoport.

- Lehetséges támadások:
  - DDOS – az oldal elérhetetlenné tétele
  - SQL-injection – az oldal adatbázisának módosítása, hozzáférések megszerzése, jelszavak esetleg ügyféladatok biztonságának sérülése.
  - Egyéb hiányosságok kihasználása
    - weboldal lecserélése tetszőleges tartalomra
    - Kártékony kódok, vírusok elhelyezése az oldalon: pl a kondíciós listák helyett vírusos állományok
    - Netbank (pl.: Electra webserver) bejelentkező felületének lecserélése (adathalászat)

Kockázatok a Takarékszövetkezetre nézve

- Az oldal adminisztrátori jogait megszerezve annak tartalmát könnyedén módosíthatják, az azon lévő speciális hozzáféréseket megszerezhetik, jelszavakat, telefonszámokat és email címeket szerezhetnek meg.

- A fenti megszerzett adatok birtokában hamis személyazonosságot alkotva maguknak az ügyfelektől adatokat, jelszavakat, pénzt szerezhetnek (Social Engineering)

- Szinte észrevehetetlen kártékony kódokat az oldalra rejtve – vírusokat (troyan horse, keylogger) telepítve így az ügyfél számítógépére – adatokat szerezhet az ügyféltől (netbank jelszó például).

- A főoldal lecserélése egy sajátra presztízsbeli kockázatot jelent. Például: trágár, rágalmazó szövegek és képek elhelyezése.

Kockázatok a Takarékszövetkezetre nézve

- Hol van a weblapot működtető szerver elhelyezve?
  - biztonságos szerverpark
    - Dedikált szerver
    - Saját szerver
  - Takarékszövetkezet belső szerverközpontja
    - Tűzfal
    - Internethozzáférés és a belső hálózattól történő szeparációja
- Ki készítette a weblapot?
  - Webfejlesztéssel foglalkozó cég
  - Honlapépítéssel megbízott személy
- Milyen programozási nyelven íródott a weblap
- Van-e bármilyen üzletviteli alkalmazás használatban a honlapon?

Védekezési lehetőségek

- Az ismert hiányosságok kiküszöbölése, a felhasználói hozzáférések minimalizálása.
- Szerver megfelelő védelme, külső hozzáférések korlátozása (távoli elérés, adatbázis szerver)
- Adminisztrátori fiókok korlátozása (csak az kapjon a ilyen jogot akinek szüksége is van rá)
- Adminisztrátorként csak az lépjen és csak akkor amikor arra szükség van
- DDOS támadások (túlterheléses támadások) elleni védelmet a szerver megfelelő hardveres és szoftveres védelme képes kezelni (nagyrészt védhetetlen). Valós kárt ritkán okoz.

Védekezési lehetőségek

- Brute force támadások kivédése: minden esemény naplózása, a belépési kísérletek korlátozása, IP cím figyelése.
- Az adminisztrációs felület valósítsa meg felhasználói tevékenységek naplózását és ezen naplók sérthetetlenségét.
- A honlap biztonsága legyen külső vállalatokkal auditálva.

Köszönöm figyelmüket!

Munkavédelem

Előadás vázlata:

- szervezeti változások
- kockázatértékelést érintő törvényi változások,
- gépek, kéziszerszámok vizsgálatának szükségessége,
- ÁNTSZ vizsgálatai, a dohányzóhelyek kijelölésének szabályai,

Szervezeti változások

- Országos Munkavédelmi és Munkaügyi Főfelügyelőség (OMMF)
- Nemzeti Szakképzési és Felnőttképzési Intézet (NSZFI)

Nemzeti Munkaügyi Hivatal

(2012. január 1.)

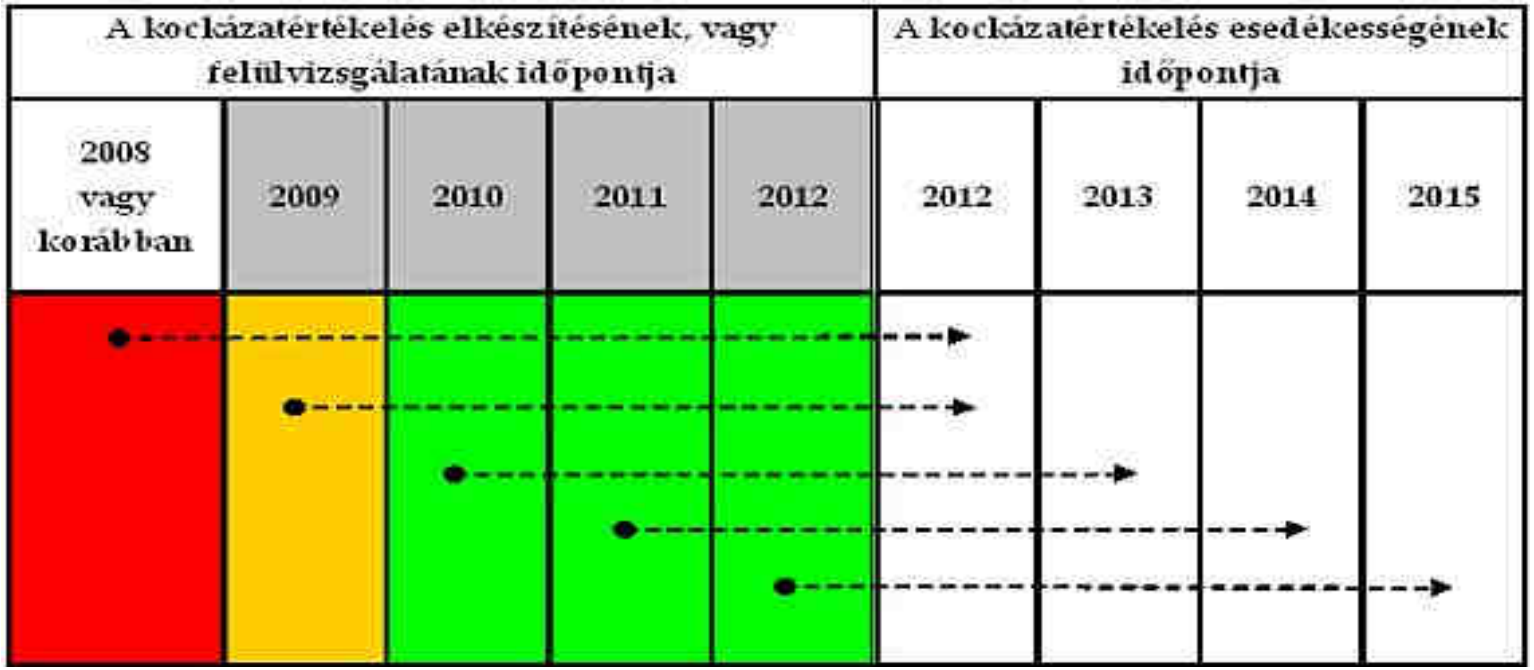
- Munkavédelmi és Munkaügyi Igazgatóság
- fővárosi és megyei kormányhivatalok munkavédelmi és munkaügyi szakigazgatási szerve (munkavédelmi és munkaügyi felügyelőség)

ÁNTSZ

- megyei kormányhivatalok népegészségügyi szakigazgatási szervei
- kistérségi népegészségügyi intézetek

Kockázatértékelést érintő törvényi változások

- A kockázatértékelés gyakorisága:
  - a munkáltató a tevékenység megkezdése előtt
  - azt követően indokolt esetben,
  - de legalább 3 évente köteles elvégezni
  - éves felülvizsgálatok elvégzése nem kötelező



A kockázatértékelés tartalmi változásai

- elsősegély-nyújtás,
- dohányzóhelyek és tűzvédelmi szabályok teljesülése
- elektromos kéziszerszámokkal végzett tevékenységek
  - Használatának rendje
    1. EK megfelelőségi nyilatkozat
    2. üzemeltetési dokumentáció
    3. szerszámgépek használatának általános szabályai
    4. munkaruházat
    5. időszakos ellenőrző felülvizsgálat jegyzőkönyve

A dohányzóhelyek kijelölésének szabályai

- 2012. január 1-től változott a nemdohányzók védelméről és a dohánytermékek fogyasztásának, forgalmazásának egyes szabályairól szóló 1999. évi XLII. törvény

- TILOS A DOHÁNYZÁS!
  - közforgalmú intézmények zárt légterű helyiségeiben
  - piktogram szükséges bejárati ajtóra vagy szélfogóra

- DOHÁNYZÁSRA KIJELÖLT HELY!
  - csak nyílt légtérben
  - piktogram szükséges
  - az alkalmazottak részére
  - bejárattól 5 m-es távolságon kívül (hátsó udvar, kert, erkély is lehet)
  - egészségügyi szolgáltatást igénybevevők útvonalától különüljön el

Az ellenőrzések tapasztalatai

- ÁNTSZ, munkavédelmi felügyelőség és a katasztrófavédelmi kirendeltség (tűzoltóság), mint ellenőrző hatóságok

- Bírságok összege 2012. április 1-től :
  - 20 000-50 000 Ft

    dohányzással összefüggő tilalmak, korlátozások megsértése
  - 100 000-250 000 Ft

    a dohányzó helyek kijelölésére vonatkozó kötelezettség nem vagy nem megfelelő teljesítése

    a dohányzást érintő tilalmak, korlátozások megtartására vonatkozó ellenőrzési kötelezettség elmulasztása

    az ellenőrzési kötelezettségek betartásáért felelős személy
  - 1 000 000-2 500 000 Ft az üzemeltető tekintetében

Köszönöm figyelmüket!

A fogyasztóvédelemről általánosságban

A fogyasztóvédelemmel kapcsolatos legfontosabb jogszabályok

- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról

- 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (XXIX. fejezet)

A **Hpt**. két jelentősebb módosítása:

- Ügyfélvédelem:
  - 199. § (1) – (3) bek. - teljes hiteldíj mutató **(THM)** mértékének maximalizálása – hatályos 2012. április 1. napjával
- Üzletszabályzat:
  - 210/B. § (1) – (10) bek. - a fogyasztóval, ingatlanon alapított jelzálogjog fedezete mellett kötött kölcsönszerződés **(jelzáloghitel-szerződés)** szabályai – hatályos 2012. április 1. napjával

A fogyasztóvédelemmel kapcsolatos legfontosabb jogszabályok

- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- 2008. évi XLVII. törvény a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról
- 2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól
- 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról
- 2009. évi CLXII. törvény a fogyasztóknak nyújtott hitelről
- 2010. évi CLVIII. törvény a Pénzügyi Szervezetek Állami Felügyeletéről

A fogyasztóvédelemmel kapcsolatos legfontosabb jogszabályok

- 2011. évi LXXV. törvény a devizakölcsönök törlesztési árfolyamának rögzítéséről és a lakóingatlanok kényszerértékesítésének rendjéről
- 2011. évi CXXI. törvény az otthonvédelemmel összefüggő egyes törvények módosításáról
- 2011. évi CXXX. törvény az otthonvédelmi intézkedések kiterjesztése kapcsán a hitelintézetekről és a pénzügyi vállalkozásokról szóló 1996. évi CXII. törvény módosításáról
- 2011. évi CXLVII. törvény az otthonvédelmi intézkedésekkel kapcsolatos egyes törvények módosításáról
- 2011. évi CXLVIII. törvény a kölcsönök kamatai és a teljes hiteldíj mutató korlátozása, valamint az átlátható árazás biztosítása érdekében egyes pénzügyi tárgyú törvények módosításáról (Hpt. mód.)
- 2011. évi CXCIII. törvény a befektetési alapkezelőkről és a kollektív befektetési formákról (a 2011. évi CXLVIII. törvény hatálybalépését is módosította)
- 2012. évi XVI. törvény a devizakölcsönök árfolyamának rögzítéséről és a lakóingatlanok kényszerértékesítésének rendjéről szóló 2011. évi LXXV. törvény módosításáról

A fogyasztóvédelemmel kapcsolatos legfontosabb jogszabályok

- 18/1999. (II. 5.) Korm. rendelet a fogyasztóval kötött szerződésben tisztességtelennek minősülő feltételekről
- 361/2009. (XII. 30.) Korm. rendelet a körültekintő lakossági hitelezés feltételeiről és a hitelképességi vizsgálatról
- 82/2010. (III. 25.) Korm. rendelet a betéti kamat és az értékpapírok hozama számításáról és közzétételéről
- 83/2010. (III. 25.) Korm. rendelet a teljes hiteldíj mutató meghatározásáról, számításáról, közzétételéről
- 275/2010. (II. 28.) Korm. rendelet a szerződésekben előírt kamat egyoldalú módosításának feltételeiről
- 341/2011. (XII. 29.) Korm. rendelet az otthonteremtési kamattámogatásról
- 57/2012. (III. 30.) Korm. rendelet a devizakölcsönök törlesztési árfolyamának rögzítését érintő megtérítéséről és a közszférában dolgozók támogatásáról

Felügyeleti elvárások

- „A fogyasztóvédelmi szempontok … most sokkal fajsúlyosabban érvényesülnek...” Szász Károly, PSZÁF elnöke

  (PSZÁF Hírlevél, 2012. március)

- A PSZÁF fogyasztóvédelmet érintő legfontosabb szabályozói:
  - A Pénzügyi Szervezetek Állami Felügyeletének 15/2001. számú ajánlása a fogyasztók pénzügyi szervezetek általi tájékoztatásáról
  - 19/2011. (X. 20.) PSZÁF rendelet a hitelintézetek adatszolgáltatási kötelezettségéről
  - 26/2011. (XI. 24.) PSZÁF rendelet a hitelintézetek és pénzügyi vállalkozások által forgalmazott termékek meghatározott körére vonatkozó adatszolgáltatási kötelezettségről
  - 28/2011. (XII. 5.) PSZÁF rendelet a hitelintézetek **befektetési szabályzatáról**

PÉNZÜGYI SZERVEZETEK ÁLLAMI FELÜGYELETE

Felügyeleti elvárások

- A Pénzügyi Szervezetek Állami Felügyelete elnökének **1/2011. (IV. 29.) sz. ajánlása** a pénzügyi szervezetek számára az általános fogyasztóvédelmi elvek alkalmazásáról
  - a PSZÁF és a pénzügyi szervezetek konzultációjának eredményeképpen létrejött ajánlás, amely megfogalmazza a **Felügyelet alapvető elvárásait** a fogyasztói érdekek érvényesítése céljából
  - A legfontosabb elvárások az **ügyfél-tájékoztatásra**, **termék-összehasonlításra**, **együttműködésre**, **átláthatóságra**, **közérthetőségre**, **panaszkezelésre**, **fogyasztói tudatosság segítésére** vonatkoznak.
- **2/2011. sz. Vezetői körlevél** a fogyasztóvédelmi ügyekért felelős kapcsolattartó feladatairól
  - A létrehozott a fogyasztóvédelmi kapcsolattartói intézmény (Hpt. 215/B. §) **feladatait**, **felelősségeit** határozza meg, egyben a fogyasztóvédelem részterületeire vonatkozó fogalmaz meg.

PÉNZÜGYI SZERVEZETEK ÁLLAMI FELÜGYELETE

Melyek az első lépések?

- A 2/2011. (IV. 29.) sz. elnöki ajánlásban meghatározott elvek és elvárások **összevetése** a takarékszövetkezet működési elveivel.
- A fogyasztóvédelmi körbe tartozó **jogszabályok**, a felügyeleti és egyéb **elvárásoknak** a Takarékszövetkezet **működési rendszerébe** történő **implementálása**,
- valamint az intézmény valamennyi **belső szabályozásának és eljárásrendjének** áttekintése és **felülvizsgálata** annak érdekében, hogy azokban a fogyasztóvédelmi körbe tartozó jogszabályi előírások, a felügyeleti és egyéb elvárások **megfelelően tükröződjenek**.
- Ez jelenti a szabályok ismeretét, és folyamatos nyomon követését (compliance), másrészt a belső szabályozó anyagok és a **gyakorlat** összhangját.

  - Szabályozási politika (elvek meghatározása)
  - Szabályozási stratégia (célok megjelölése)
  - Szabályzat (jogszabálynak megfelelően)
  - Eljárásrend (az ügymenet leírása)

És hogyan tovább?
A fogyasztóvédelmi kapcsolattartó és feladatai

- A kapcsolattartó személyével szembeni felügyeleti elvárások:
  - Kellő felhatalmazással és támogatással rendelkező legyen
  - Független legyen
  - A belső ellenőrrel és a compliance feladatokat ellátó személlyel együttműködve végezze feladatát
  - (A kijelölt személy munkaköri leírásában jelenjenek meg a fogyasztóvédelmi kapcsolattartói feladatok, valamint az SZMSZ-ben is kerüljön feltüntetésre a pozíció.)
- A Felügyelet kizárólag a kijelölt személlyel tartja a kapcsolatot. Fontos, hogy az aktuális adatok álljanak a PSZÁF rendelkezésére.

És hogyan tovább?
A fogyasztóvédelmi kapcsolattartó és feladatai

Koordináló, az alábbi feladatokat összefogó szerepe van a fogyasztóvédelmi kapcsolattartónak:

- A jogszabályoknak, a felügyeleti és egyéb elvárásoknak megfelelő **egységes gyakorlat kialakítása** (szabályzat, monitoring)
- Folyamatos **jogszabálykövetés** (az újdonságok elérhetővé tétele)
- A fogyasztóvédelmi elvárásoknak való **megfeleltetés** az új termékek, eljárásrendek kialakítása során
- **Panaszkezelési gyakorlat** monitoringja
- Felügyeleti **adatszolgáltatás** (megfelelő tartalommal, és határidőben)
- **Ügyfél-tájékoztatás** és kapcsolattartás eredményességének mérése
- **Munkatársak oktatása** (legyen felkészült az ügyintéző is)
- A **tudatos fogyasztói szemléletmód** fejlesztése (honlap, hirdetőtábla)

Gyakorlati tapasztalatok

A fogyasztóvédelmi kérdőív, illetve helyszíni egyeztetés tapasztalatai:

- A **kapcsolattartó személye** megfelelően lett kijelölve, azonban a munkaköri leírások nem mindig követik le a változásokat.
- A **belső szabályzatok** a jogszabályi előírásoknak megfelelően módosításra kerültek, illetve kerülnek. Az eddigi tapasztalatok szerint fogyasztóvédelmi szabályzattal is rendelkezik a Takarékszövetkezetek többsége.
- A **jogszabálykövetés** megvalósul, van ahol központi rendszeren elérhetőek az aktuális szabályozók, míg másutt folyamatosan figyelik és frissítik a szabályozók jegyzékét.
- **Tájékoztató anyagok** a termékekkel kapcsolatosan rendelkezésre állnak. Az egyoldalas tájékoztatók még nem mindenütt jelentek meg.

Gyakorlati tapasztalatok

A fogyasztóvédelmi kérdőív, illetve helyszíni egyeztetés tapasztalatai:

- A **panaszok dokumentálása** megtörténik, és éves jelentés készül a vezetőség felé.
- **Ügyfél-elégedettség** mérése – több helyen kérdőíves formában megtörtént (pozitív visszajelzéseket kaptak a Takarékszövetkezetek, és ügyféligények is megfogalmazódtak)
- A **munkatársak** éves **oktatása** igazolt (jelenléti ív), a speciális oktatások esetében ez helyenként hiányzik. Általánosan elmondható, hogy a számonkérés dokumentáltan nem történik meg.
- A **fogyasztók tájékozottságának elősegítésére** a Felügyelet fogyasztói oldala elérhető a takarékszövetkezeti honlapokon, és a hirdetőtáblákon ezzel kapcsolatos tájékoztató anyagok fellelhetőek az ügyfelek számára.

Gyakorlati tapasztalatok

- A **Felügyelet** 2011. II. féléves fogyasztóvédelmi célú hatósági tevékenységének **tapasztalatai** alapján kiemelt figyelmet kell tanúsítani:
  - **Panaszkezelési határidők** betartására
  - **Időszakos tájékoztatási kötelezettség** teljesítésére (egyértelmű, közérthető és teljes körű elszámolás)
  - **Tisztességes kereskedelmi gyakorlat** folytatására
  - **Banktitok** megtartására
  - **KHR** ügyfélvédelmi rendelkezések betartására
  - A **Pénzügyi Békéltető Testülettel** való együttműködési kötelezettségre
  - **Belső csalások** megelőzésére tett intézkedésekre

Köszönöm a figyelmüket!

Pénzmosás-megelőzés

Adminisztratív változások (2012.01.01-től)

- 2012. január 1-től megváltozott a Pmt. szerinti pénzügyi információs egységként működő hatóság neve és szervezetileg is függetlenné vált: a Bűnügyi Főigazgatóság helyett a Központi Hivatal alá tartozik a Pénzmosás Elleni Információs Iroda (a továbbiakban: PEII)

  [273/2010 (XII.9.) Korm. rendelet 41.§]

- Az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény (2007. évi CLXXX. törvény) szerinti pénzügyi és vagyoni korlátozó intézkedés foganatosításáért felelős szervként szintén a PEII került meghatározásra.

- Pénzeszközök átutalására vonatkozó korlátozó intézkedés foganatosításáért szintén a PEII a felelős.

  [273/2010 (XII.9.) Korm. rendelet 41.§]

- A bejelentések felhasználásánál az adócsalás tényállása helyett költségvetési csalás szerepel a Pmt-ben.

A várható jogszabályi változásokról (tervezet)

- Az Európa Tanács Pénzmosás Elleni Bizottsága (Moneyval) által megfogalmazott ajánlások alapján az alábbi változások várhatók:
  - A pénzmosás és a terrorcselekmény törvényi tényállásának változása (Btk. 303.§; 303/A.§ illetve 261.§)
  - Új mintaszabályzat várható a felügyeleti szervek részéről
  - Tényleges tulajdonos törvényi meghatározása és a rá vonatkozó azonosítási kötelezettség változtatása (tényleges tulajdonosi nyilatkozat)
  - Bejelentési kötelezettség kiterjesztése: jelenteni kell, ha az ügyfél-átvilágítás valamely okból nem hajtható végre; adózáshoz köthető bűncselekmények jelentése; megkísérelt, de nem teljesült ügyletek jelentése
  - Képviseleti jogosultság szigorúbb ellenőrzése a személyazonosság igazoló ellenőrzése során
  - Kötelező fokozott ügyfél-átvilágítási intézkedések (maximum adatkörön felül)

A várható jogszabályi változásokról (tervezet)

- Kötelező fokozott ügyfél-átvilágítási intézkedések (maximum adatkörön felül)
- A politikai közszereplő (PEP) törvényi meghatározásának változtatása a nemzetközi követelményekkel összhangban
- A pénzmosás-megelőzési szabályok megsértése esetén alkalmazandó intézkedések szélesebb körben való alkalmazása a pénzügyi szolgáltatók vonatkozásában (magasabb összegű bírság, engedély visszavonása)
- Az ügyleti megbízások hatósági jogkörben történő felfüggesztése lehetővé tételének vizsgálata
- A szolgáltatók által alkalmazott felfüggesztés időtartamának felülvizsgálata (hosszabbítás lehetősége)
- Szankciós listák használatának koordinálására, terjesztésére vonatkozó lehetőségek vizsgálata.

Monitoring és szűrőrendszer

- A Takarékszövetkezetnek az üzleti kapcsolatot folyamatosan figyelemmel kell kísérnie, annak megállapítása érdekében, hogy az adott ügyleti megbízások összhangban vannak-e az ügyfélről rendelkezésre álló adatokkal. Hozzátartozik a korábban teljesített ügyleti megbízások elemzése is.
- A szokatlan tranzakciók esetén – ha szükségesnek mutatkozik - meg kell tenni a bejelentést a kijelölt személy segítségével.
- Szokatlan pl. ügyfél portfóliójának hirtelen, szokásos gazdasági eseménnyel nem magyarázható változása; ügyfélprofilba nem illeszkedő ügylet; a tranzakciónak nincs ismert, elfogadható indoka, napon belül nyújtott folyószámla-hitelek ellenőrzése (folyószámla túlhívás, a hitelösszeg zárt, egymással tulajdonosi és finanszírozási kapcsolatban álló társaságok közötti körbeutalása).
- A Felügyelet elvárása a paraméterezhető szűrőrendszer, hogy a jogszabályi előírások változása esetén ne kelljen új rendszert létrehozni, a meglévőt kelljen csak változtatni.

Ügyfélprofil

- Az ügyfél gondos megismerése, pénzügyi, fizetési szokásainak, kapcsolatainak, pénzforgalmának megfelelő nyilvántartása annak érdekében, hogy vizsgálható legyen, az ügyfél üzleti és kockázati jellemzői összhangban állnak-e a kezdeményezett ügyleti megbízásokkal.
- A nem honos kirendeltségek számára biztosítani kell, hogy az ügyfélprofil elérhető legyen – informatika segítségével, vagy egyéb módon.
- Szűrés:
  - Ügyintézők általi napi lista-ellenőrzés
  - Kirendeltség-vezetők általi napi lista-ellenőrzés
  - Központi számviteli munkatársak általi ellenőrzés
  - Ügyfél – és tranzakciós adatok meghatározott csoportjára nézve végzett szűrés

Ügyfélprofil

- Ügyfélkategóriák:
  - Természetes személy
  - Egyéni vállalkozó
  - Társas vállalkozás
  - Nonprofit és egyéb kis kockázatú szervezet
  - Külföldi érdekeltségű személyek és szervezetek

- További alkategóriák is képezhetők a fentieken belül:
  - Forgalom nagysága szerint (pl. átlagos forgalmú természetes személy – 500 ezer és 1 millió között)
  - Tranzakciók száma szerint (max. 20 tranzakció havonta)
  - Tranzakció típusa szerint (sok készpénzfelvétel, egy-két utalás)

- Pl. kisforgalmú, átlagos forgalmú és VIP természetes személy kategória

Ügyfélprofil

- Paraméterek
  - Készpénzbefizetés forgalom
  - Készpénzfelvétel forgalom
  - Utalás érkező forgalom
  - Utalás kimenő forgalom
  - Pénzváltás
  - Tranzakciószám kifelé
  - Tranzakciószám befelé
  - Tranzakció külföldre összeg
  - Tranzakciószám külföldre
  - Külföldről érkező összeg
  - Nagyobb összegű tranzakciók száma (állítható összeggel)
  - Átlagos forgalom (havi szinten; tranzakciók összege/darabszám)

Havi lebontásban ellenőrizhetők a paraméterek. Ha több egymást követő hónapban is a kategóriától eltérő paraméterek mutatkoznak – vizsgálat.

Ügyfélprofil

Példa:

- Természetes személy, aki legfeljebb 500-500 ezer forint forgalmat bonyolít havonta, 15-20 tranzakció legfeljebb, kisebb összegű pénzfelvételek, nincs külföldi mozgás.
- Amennyiben a beállított kategóriának megfelelő paraméterektől eltér az ügyfél több ponton, vagy többször egymás után, a Takarékszövetkezet felülvizsgálja a besorolását és adott esetben eggyel kockázatosabb kategóriába helyezi(pl. kisforgalmúból a normálba)
- Ehhez az informatikai rendszerben be kell állítani a paramétereket az egyes kategóriákhoz, és meg kell határozni, hogy milyen esetben kell a kategóriát változtatni (pl. két hónapos eltérés után a harmadik hónapnál)
- A kategóriába való áthelyezés nem automatikus, mivel lehet olyan körülmény, amely indokolja a változást (pl. ingatlan eladásból nagyobb összeghez jutott az ügyfél) – az ügyintéző lépteti az ügyfelet, ha kell. Természetesen kétirányú a mozgás.

Ügyfélprofil (a standard paraméterekkel)

Természetes személy	
készpénz befizetés	200000
készpénz felvétel	500000
utalás érkező forgalom	500000
utalás kimenő forgalom	500000
külföldre menő forgalom	200000
külföldről érkező forgalom	500000
pénzváltás	500000
tranzakciószám kifelé	0-20
tranzakciószám befelé	0-10
tranzakciószám külföldre	0-5
tranzakciószám külföldről	0-5
nagyobb összegű tranzakció	3600000
átlagos forgalom	100000

Ügyfélprofil (eltérések, de indokolható)

Természetes személy	
készpénz befizetés	200000
készpénz felvétel	500000
utalás érkező forgalom	500000
utalás kimenő forgalom	500000
külföldre menő forgalom	200000
külföldről érkező forgalom	2000000
pénzváltás	500000
tranzakciószám kifelé	0-20
tranzakciószám befelé	0-10
tranzakciószám külföldre	0-5
tranzakciószám külföldről	3
nagyobb összegű tranzakció	3600000
átlagos forgalom	200000

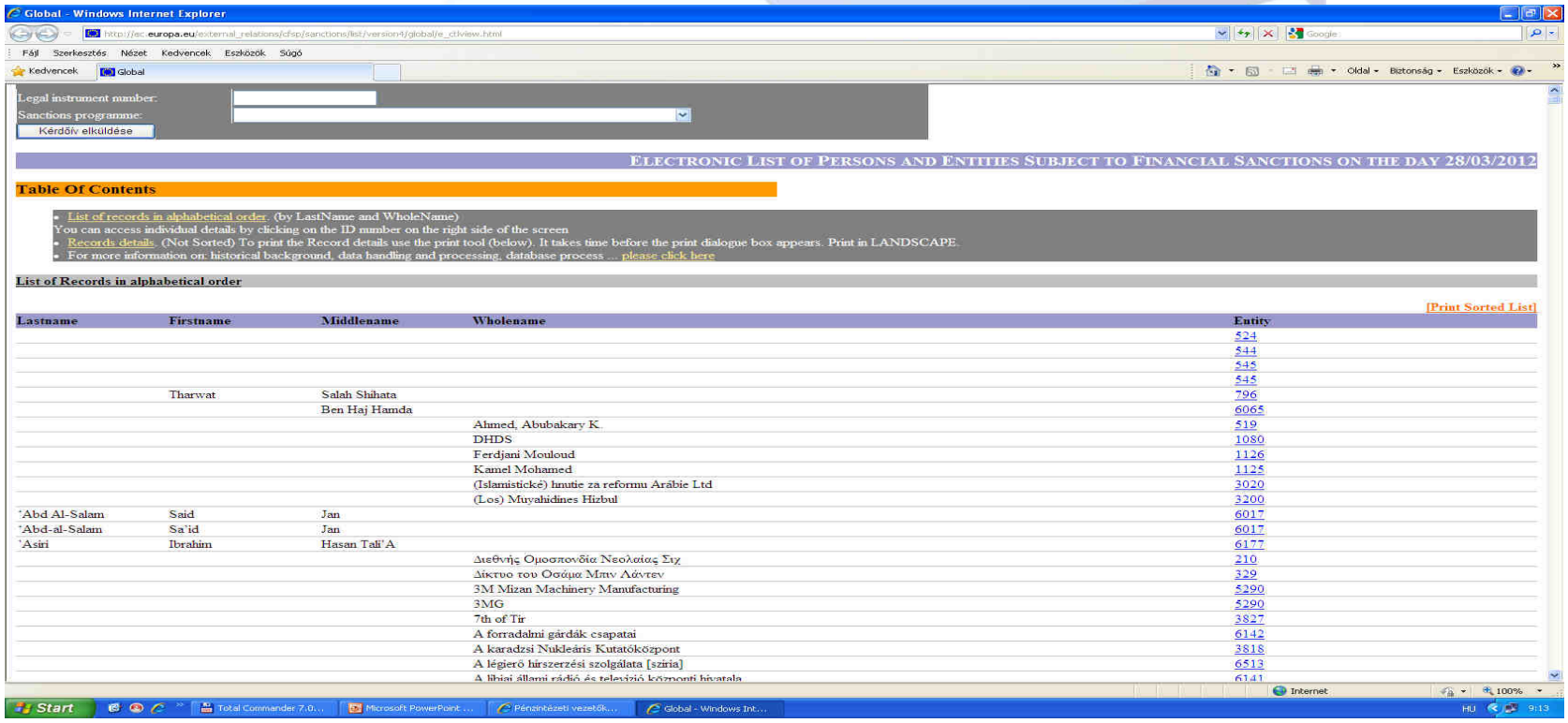
Ügyfélprofil (szokatlanság az eltérések mellett)

Természetes személy	
készpénz befizetés	200000
készpénz felvétel	500000
utalás érkező forgalom	500000
utalás kimenő forgalom	500000
külföldre menő forgalom	200000
külföldről érkező forgalom	2000000
pénzváltás	500000
tranzakciószám kifelé	0-20
tranzakciószám befelé	0-10
tranzakciószám külföldre	0-5
tranzakciószám külföldről	12
nagyobb összegű tranzakció	3600000
átlagos forgalom	200000

Szankciós lista használata

http://ec.europa.eu/external_relations/cfsp/sanctions/list/version4/global/e_ctlview.html

Az Európai Unió által elrendelt pénzügyi és vagyoni korlátozó intézkedések hatálya alatt álló természetes és jogi személyek konszolidált listája.



Szankciós lista használata

- A szankciós listán szereplő személyekkel szemben az Európai Unió adminisztratív módon történő (tehát büntetőeljárás nélküli) vagyonelvonást alkalmaz – **befagyasztás**.
- Nem végleges vagyonelvonás, csupán a vagyon feletti rendelékezési jog gyakorlásának felfüggesztése:
  - A Takarékszövetkezet köteles jelenteni, ha a listán szereplő személynek vagyoni korlátozó intézkedés hatálya alá tartozó pénzeszközéről, gazdasági erőforrásáról szerez tudomást (jelentési kötelezettség).
  - Az ügyfél által kezdeményezett tranzakció nem hajtható végre (**felfüggesztés**). Az ügyfél korlátozással érintett számlájára érkezett összeget a Takarékszövetkezet köteles **zárolni**.
  - A Hatóság ebben az esetben is: NAV Központi Hivatala Pénzmosás Elleni Információs Iroda
  - A bejelentést a Szabályzat mellékletében található nyomtatványon kell megtenni.

A PSZÁF Felügyeleti Tanácsának 3/2008. (XI.20.) számú ajánlása a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

A Felügyelet ellenőrzi, hogy a pénzügyi szervezet szabályzatában foglalt rendelkezések megfelelnek-e a Felügyeleti Tanács által kiadott jelen ajánlásnak és összeveti a szolgáltatók erre vonatkozó gyakorlatát, eltérő gyakorlat esetén felhívja a szolgáltatót az ajánlásnak megfelelő szabályozás kialakítására.

A PSZÁF ajánlás nem jogszabály, nem bír kötelező erővel, mégis meg kell felelni a benne foglalt követelményeknek:

jogszabálykövetés vs. fejlesztés

Lehet-e hivatkozni a szoftvergyártó felé a PSZÁF ajánlásaira?

Milyen következménye van, ha nem tartjuk be az ajánlásban foglaltakat?

Köszönjük figyelmüket!

www.zsigraikft.hu