Ernst & Young Kft.
Ernst & Young Ltd.
H-1132 Budapest Váci út 20.
1399 Budapest 62. Pf.632, Hungary

Tel: +36 1 451 8100
Fax: +36 1 451 8199
www.ey.com/hu
Cg. 01-09-267553

Szügyi Dániel – Schrettner Attila

Pandora Papers - compliance és belső ellenőrzés

* A nyilvánosságra hozott dokumentumok és a szivárogtatási botrányok hatása KYC folyamtokra*

I. Bevezetés

2021, október 3-án hozta nyilvánosságra az International Oknyomozó Újságírók Nemzetközi Konzorciuma (ICIJ) Consortium Of Investigative Journalists[1] a legújabb tényfeltáró munkájának eredményét Pandora-iratok néven.

A Pandora-iratok mintegy 11,9 millió dokumentumot tartalmaznak, amelyek 14 offshore szolgáltatásokat nyújtó vállalattól kerültek kiszivárogtatásra. A dokumentumok alapján 956 offshore cég azonosítható be, és ezek 336 magas rangú politikushoz[2] vagy köztisztviselőhöz köthetők[3].

A Pandora-iratok nem egyedülálló jelenség, az utóbbi években sorra jelentek meg hasonló szivárogtatások dokumentumai, főként az Oknyomozó Újságírók Nemzetközi Konzorciuma (ICIJ) gondozásában. A legjelentősebbek a FinCEN Files (2020), a Paradise-iratok („Paradise Papers", 2017), a Panama iratok („Panama Papers", 2016) és a Luxembourg Leaks (2014) voltak[4]

II. Potenciális KYC/CDD vonatkozások

Milyen hatással vannak ezek a szivárogtatások a vállalatok működésére? Miként tudják biztosítani a vállalatok, hogy a törvénysértő – jellemzően pénzmosó vagy adócsaló –, vagy etikailag megkérdőjelezhető üzleti partnerek (beleértve az ügyfeleket, beszállítókat, alvállalkozókat stb.) kiszűrhetők legyenek?

Ennek a szűrésnek az egyik területe, amely kifejezetten az ügyfelekre fókuszál az „ismerd meg az ügyfeled" (angolul: know your customer (KYC) vagy customer due diligence (CDD); a továbbiakban: „KYC/CDD"). A KYC elsősorban a pénzmosás területéről lehet ismerős, de azon cégek számára is érdemes lehet megfontolni valamilyen szintű KYC/CDD alkalmazását, amelyek nem esnek a Pmt.[5] hatálya alá. A meglévő szűrés frissítése vagy egy egyszerű KCY/CDD szűrés bevezetése is elegendő lehet a legkockázatosabb ügyfelek kiszűrésére.

Itt fontos megjegyezni, hogy a Pandora-iratok és a korábbi szivárogtatások által azonosított személyek és cégek nem feltétlenül követtek el törvénytelen vagy etikátlan cselekedet, illetve vagyonuk nem feltétlenül származik ilyen forrásból. Mindez ugyanis csupán egy *„red flag"*, amelyből legfeljebb annyi derülhet ki, hogy mennyi és milyen vagyont birtokol az adott személy bizonyos off-shore cégeken keresztül[6]. Minden esetben tehát további mérlegelés szükséges.

---

[1] Link: https://www.icij.org/

[2] Guardian investigations team (2021): Pandora papers: biggest ever leak of offshore data exposes financial secrets of rich and powerful, Guardian; Link: https://www.theguardian.com/news/2021/oct/03/pandora-papers-biggest-ever-leak-of-offshore-data-exposes-financial-secrets-of-rich-and-powerful

[3] Link: https://www.icij.org/investigations/pandora-papers/global-investigation-tax-havens-offshore/

[4] Link: https://www.icij.org/investigations/

[5] 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról

[6] Arabella Murphy (2021): Pandora Papers: In defence of offshore trusts, Spear's; Link: https://www.spearswms.com/pandora-papers-in-defence-of-offshore-trusts/

A meglévő szűrések jellemzően három okból lehetnek kevésbé hatékonyak[7]:

- **Eltérő adatok:** A friss és „*legacy*" rendszerek[8] között gyakran inkonzisztencia léphet fel. Nem is beszélve az esetlegesen több országban jelen lévő, több terméket igénybe vevő, vagy bonyolult tulajdonosi struktúrával rendelkező ügyfelekről, amelyek esetében ezek – az egyes rendszerek adattartalmában jelentkező - eltérések még jelentősebbek lehetnek. Így előfordulhat az, hogy a központ kockázatosnak minősít egy a Pandora-iratokban említett ügyfelet, de a leányvállalat rendszereiben ez nem képződik le.

- **Manuálisan intenzív folyamatok:** A nagy mennyiségű manuálisan intenzív feladatok esetében magas arányban fordulhatnak elő hibásan rögzített adatok. A javításuk egyfelől extra erőforrást igényel, másrészt a javítás elvégzéséig az adatok hibás képet adnak az adott ügyfélről. A hibás adatok alapján hibás döntés születhet, és olyan ügyfelek is „házon belülre" kerülhetnek, amelyek egyébként a vállalat kockázati étvágyába már nem férnek bele, így például a Pandora-iratokban előforduló személyek.

- **Papír alapú dokumentumok:** Gyakran a KYC/CDD során az adatok papír alapú dokumentumokon, pl.: nyilatkozatokon kerülnek felvételre. Ha ezek nem kerülnek megfelelően digitalizálásra, akkor egy nehezen kezelhető és lassan kereshető információ halmaz jön létre, amely lassíthatja az üzleti működést. Ezen felül komplexebb döntéselőkészítő statisztikák, kimutatások sem készíthetők az összegyűjtött információkból. Mindezek eredménye az lehet, hogy a vállalat nem lesz képes kiszűrni a kockázatos ügyfeleket.

Egy új és egyszerű KYC/CDD szűrés bevezetése esetén érdemes néhány kulcs elemre odafigyelni:

- **Célok meghatározás:** A vállalatnak el kell döntenie, hogy pontosan milyen kockázatokat akar kiszűrni a KYC/CDD folyamat során. A leggyakoribbak a szankciós, pénzmosási, csalási vagy reputációs kockázatok lehetnek[10]. Ezeken belül a Pandora-iratok kapcsán leginkább a pénzmosás és az adócsalás kerülhet fókuszba.

- **Megfelelő adatforrások összegyűjtés:** A vállalatnak ki kell jelölnie, hogy milyen forrásokat kíván felhasználni a KYC/CDD szűrés során. Ezek lehetnek nyilvános és zárt, harmadik féltől vásárolt adatforrások, illetve ahogy a vállalat egyre nagyobb rutint szerez a KYC/CDD szűrésben, úgy saját belső listákat is összeállíthat[9].

- **Felelős személy kijelölése:** Célszerű kijelölni a vállalaton belül egy személyt, aki felel a KYC/CDD szűrésért, és összefogja az ehhez a területhez kapcsolódó feladatokat.

- **Munkavállalók képzése:** A KYC/CDD szűrést konkrétan végző munkavállalókon túl érdemes lehet a vállalat valamennyi munkavállalóját képezni. Ezáltal kialakulhat egy tudatos kultúra a törvénysértő vagy etikátlan ügyfelek kiszűrésére akkor is, ha azok esetleg nem kerültek be a KYC/CDD szűrésbe, azonban valamelyik munkavállaló észleli az ügyfél kockázatos jellegét.

- **Vezetői jelentés:** Fontos elem továbbá, hogy a vállalat vezetősége rendszeres időközönként vagy jelentős kockázati események esetén jelentést kapjon a KYC/CDD szűrések eredményeiről, illetve magának a szűrésnek a

[7] EY (2020): How to get ready for dynamic, continuous KYC
[8] Itt: Régi, ismeretlen vagy elavult belső technológiával működő hasznos rendszerek
[9] Link: https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd

hatásosságáról és hatékonyságáról. Így a vezetőség naprakész adatok alapján tudja alakítani a kapcsolódó folyamatokat és kontrollokat.

III. Belső ellenőrzés szerepe a KYC/CDD területén

Miként biztosítható, hogy a KYC/CDD rendszer hatékonyan, az üzleti működést nem gátolva működjön? Itt léphet be a belső ellenőrzés, amely vizsgálni tudja a KYC/CDD szűrést a jogszabályoknak, a vállalat belső szabályzatainak tükrében, valamint a szűrés egyéb vonatkozásairól is független, belső véleményt tud kialakítani.

Ennek keretében a belső ellenőrzés vizsgálhatja, hogy a vállalat szabályzatai, eljárásrendjei vagy folyamatai megfelnek-e a kitűzött céloknak, hogy a munkavállalók megfelelően hajtják-e végre a szabályzatokat, eljárásrendeket és folyamatokat, hogy a KYC/CDD szűrés (és a második védelmi vonal ellenőrzései) mennyire hatékony, valamint, hogy a képzések milyen hatást fejtenek ki a munkavállalókra[10]. Ezeken az alapvető teszteken felül bármilyen más vizsgálat is szóba jöhet, amely a vállalat compliance célkitűzéseihez kapcsolódik.

Fontos ellenőrzés lehet – amennyiben a vállalat kockázat alapú megközelítést (*„risk based approach"*) alkalmaz – az egyes partnerek kockázati besorolásának és a besorolás módszertanának ellenőrzése is. Az egyes kockázati kategóriákból ugyanis teljesen más intézkedések következhetnek. Így például, ha Pandora-iratokban való előfordulás miatt a vállalat magas kockázati kategóriába sorol egy adott partnert, ezáltal sokkal szigorúbb nyomon követést és biztosítékokat követelhet meg a kapcsolódó tranzakciókra vonatkozóan, valamint magasabb szintű vezetői döntéshez kötheti azokat.

Érdemes kiemelni, hogy a KYC/CDD szűrést rendszeres időközönként meg kell ismételni, nem elegendő a partnerrel történő kapcsolatfelvétel során történő ellenőrzés. Így feltárható, ha valamely partner neve felbukkan egy újabb kiszivárgott dokumentum csomagban, és ennek megfelelően módosítható a kockázati besorolása a vállalat kockázati étvágya szerint.

IV. Összefoglaló

A Pandora-iratok és más nyilvánosságra került dokumentumok segíthetnek kockázati indikátorként felfedni a vállalatok számára a kockázatosabb ügyfeleket, ez azonban csak akkor érhető el, ha a KYC/CDD szűrés megfelelően működik, és a belső ellenőrzés is kellő alapossággal vizsgálja a területet. Ha ezek mind a helyükön vannak, akkor viszont számtalan kockázattól óvhatják meg a vállalatot. Ha egyes speciális témákban nem áll rendelkezésre ehhez kellő belső szakértelem, akkor a felsővezetés és a felügyelő bizottság erről való tájékoztatása mellett érdemi támogatásuk kérése szükséges.

Ennek keretében akár megfelelő szakértelmű külső feleket is be kell bevonjanak a compliance keretrendszer és a KYC/CDD szűrés hatékonyságának és hatásosságának értékelésébe és az ennek elvégzéséhez, valamint az ennek nyomán szükséges fejlesztések anyagi- és emberi erőforrásának biztosítása érdekében.

[10] Basel Committee on Banking Supervision (2017): Guidelines: Sound management of risks related to money laundering and financing of terrorism, Link: https://www.bis.org/bcbs/publ/d405.pdf