JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

*„A fickó beszélne, de nem teheti.”*

# A whistleblowing jogi szabályozása a magánszektorban

Szerző:

**Dr. Domokos N. Márton**

Budapest,

2013. december 31.

A „fickó” Jeffrey Wigand – az egyik leghíresebb whistleblower, a Brown & Williamson dohánycég volt kutatási és fejlesztési alelnöke, aki a CBS tévécsatorna hírműsorában (60 Minutes) leplezte le volt munkáltatójának a cigarettában található nikotin mennyiségével kapcsolatos jogellenes manipulációit. Azt pedig, hogy miért is nem beszélhet, a nagyközönség számára Michael Mann 1999-es, „A bennfentes” (The Insider) című filmje mutatta be, ahol Russell Crowe Oscar-díjra jelölt alakítással küzdött a komplex titoktartási szerződések és a névtelen fenyegetések ellen.

Jeffrey Wigand története persze csak egy az USA-ban már részletes jogszabályi háttérrel védett és motivált whistleblowing eljárások közül. A whistleblowing rendszerek (belső visszaélés-jelző / visszaélés-jelentési rendszerek) lényege, hogy egy vállalat munkavállalói speciális belső eljárásrendszeren keresztül, egy erre szakosodott szolgáltató (például ügyvéd) vagy erre elkülönített belső részleg számára bejelentést tehetnek a vállalaton belül tudomásukra jutott kötelezettségszegésekről, jogszabálysértésekről. A speciális eljárási rend arra az esetre kerül bevezetésre, ha egy munkavállaló nem akarja igénybe venni a munkaszervezeten belül a „hagyományos”, nyilvános jelentéstételi / panasztételi eljárást, mert fél a panasszal érintett munkatársak, vezetők retorziójától, vagy a panasztétellel járó nyilvánosságtól, de az is hátrányos lehet számára, ha az iparágban elterjed, hogy miatta került nyilvánosságra egy egyébként mindenki által ismert és hallgatólagosan elfogadott jogszabálysértés (tipikusan ilyen a korrupció, vagy a versenykorlátozó gyakorlat). Egy jól kidolgozott whistleblowing rendszer biztosítja a bejelentő védelmét (legfőképpen a rendszerbe kerülő adatok bizalmas kezelésével és a retorziók, fegyelmi intézkedések, diszkrimináció tiltásával), valamint a bejelentési eljárás hatékony lefolytatását (pl. pontos határidőkkel, kifejezetten erre a célra kijelölt kommunikációs csatornákkal, azonnal bevonásra kerülő külső szakértőkkel) - és ezzel végső soron elősegíti az eljárás tárgyát képező jogszabályok és egyéb szabályozások megfelelő betartását.

Egy whistleblowing rendszer üzemeltetése során különösen adatvédelmi szempontból kell nagyon körültekintően eljárni: az eljárás során jelentős mennyiségű személyes adatot kezelnek (pl. munkavállalói adatok gyűjtése, tárolása, nyilvántartása, adatátadás harmadik feleknek, adatmegsemmisítés), emiatt rendkívül fontos a bejelentő adatainak bizalmas kezelése. Ha pedig egyéb érintettek (pl. más munkatársak, vagy a szabályszegéssel megvádolt személy) tudomást szereznének a bejelentő

személyazonosságáról és emiatt a bejelentőt retorziók érhetnék, vagy ha illetéktelen személyek (pl. versenytársak) jutnának az üggyel kapcsolatos adatokhoz, az éppen a whistleblowing által biztosított előnyöket kérdőjelezné meg. A tisztességes eljárás biztosításához elengedhetetlen továbbá a megvádolt személy védelme is: részletes jogokat kell számára biztosítani, hogy megismerhesse az ellene felhozott vádat, és az eljárásban megfelelően kifejthesse álláspontját és védekezhessen.

Magyarországon a munkáltatók whistleblowing rendszereiket eddig a jogalkalmazók számára is kevésbé ismert 2009-es jogszabály (a tisztességes eljárás védelméről, valamint az ezzel összefüggő törvénymódosításokról szóló 2009. évi CLXIII. törvény) és a korábbi Adatvédelmi Biztos állásfoglalásai alapján működették.[1] Nemrég azonban elfogadásra került a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény (a jelen írásban: **„Whistleblowing Törvény"**) ami hatályon kívül helyezi a 2009-es jogszabályt, valamint egységesíti és törvényi szintre emeli az Adatvédelmi Biztos legfontosabb ajánlásait. Mind a jogalkotó, mind a piaci szereplők azt várják az új törvénytől, hogy a megfelelő jogi háttér alapján az érintettek bátrabban használják majd a whistleblowing rendszereket, elősegítve ezzel a vállalatirányítási szabályoknak való megfelelést, valamint a vállalatoknál előforduló kötelességszegések vagy jogellenes gyakorlatok leleplezését, erősítve ezzel a korrupció elleni harcot és az átláthatóságot.[2] A jogszabálynak mindemellett megfelelő és gyakorlatias munkajogi- és adatvédelmi megfelelőségi előírásokat kell biztosítania a whistleblowing rendszereket működtető munkáltatók számára.

A jelen írás arra az esetkörre fókuszál, hogy a Whistleblowing Törvény alapján milyen feltételekkel üzemeltethetők a whistleblowing rendszerek Magyarországon a magánszektorban.

## I. Kitekintés – a whisleblowing nemzetközi gyakorlata

A whistleblowing eljárások a nemzetközi gyakorlatban a 2000-es évek elején az USA-ban napvilágra került számviteli- és egyéb gazdasági visszaéléseket követően – például Enron, WorldCom ügyek - váltak elfogadottá. Az említett visszaéléseket követően került elfogadásra az ún. „Public Company Accounting Reform and Investor Protection Act of 2002" (Sarbanes-Oxley Act, ismertebb nevén „SOX"),

[1] Az ezzel kapcsolatos tapasztalatokat nagyon jól összefoglalja **Liber Ádám** cikke: **A tisztességes eljárás védelme – a belső visszaélés-jelentés hazai szabályozása** (Gazdaság és Jog, 2010. április), de érdemes megemlíteni **Dr. Hegedűs Bulcsú** vonatkozó cikkeit is a Collega 2007. 2-3. (**A belső visszaélés-jelentési rendszerek alkalmazása - az adatvédelem tükrében**) és a Munkaügyi Szemle 2007. 5. számában (**A belső visszaélés-jelentési rendszerek magyarországi alkalmazása**).

[2] Nem véletlen, hogy a whistleblowing rendszerekkel kapcsolatos szabályozást Magyarországon elsősorban non-profit szervezetek kutatták, úgymint **TASZ**, **Transparency International** és **K-Monitor**; a legfontosabb projektet és a kapcsolódó tanulmányokat lásd: http://www.whistleblowing-cee.org/countries/hungary/research/, illetve http://www.whistleblowing-cee.org/summing-study/

mely az USA-ban tőzsdére bevezetett cégek számára kötelezően előírta etikai kódexek, valamint bizalmas és névtelen bejelentési eljárások bevezetését. A jogszabály rögzítette továbbá, hogy a munkavállalókat nem érheti hátrány a bejelentési-eljárás használata miatt, és aki ilyen hátrányt okoz, akár 10 év szabadságvesztéssel és pénzbüntetéssel is büntethető. A „Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" nevű jogszabály ennél is tovább ment: a jogellenes tevékenységet leleplező információk bejelentéséért – ha a bejelentés alapján az USA Értékpapír- és Tőzsde Felügyelete (U.S. Securities and Exchange Commission – „SEC") sikeresen jár el az elkövetővel szemben – a bejelentő személyt a kiszabott bírság 10-30%-át kitevő „jutalom" illeti meg. A whistleblowing rendszerek használata az új angol antikorrupciós jogszabály elfogadása után is még jobban elterjedt: a UK Bribery Act 2010 szerint ugyanis bűncselekményt követ el az a vállalat, amelyik nem léptet hatályba megfelelő belső eljárásokat a korrupció megelőzésére – egy whistleblowing rendszer jelentős eleme lehet egy ilyen belső eljárásrendszernek.

Három tipikus whistleblowing eljárás a nemzetközi gyakorlatból: közös bennük, hogy a bejelentőt minden esetben retorzió érte a jogellenes gyakorlat jelzése miatt, és emiatt bíróságon keresett (és talált) jogorvoslatot. David P. Weber - pont a SEC munkatársa - munkaviszonyát az egyik leghírhedtebb befektési csalás (Bernie Madoff-ügy) vizsgálata során felmerülő szabálytalanságokkal, és egy, a hatóság elleni kínai hackertámadással összefüggő biztonsági hiányosságokkal kapcsolatos bejelentését követően szüntették meg.[3] Miután bíróságon keresett jogorvoslatot, volt munkáltatójával 580.000 USD értékű peren kívüli egyezséget kötöttek. Az egyik legmagasabb pozíciót betöltő whistleblower Michael Woodford, az Olympus Corporation vezérigazgatója: a társaság megszüntette munkaviszonyát, miután számlázási hiányosságokra és gyanús utalásokra hívta fel a figyelmet. Az ezt követő munkaügyi perben 10 millió GBP értékű egyezség született.[4] Whisleblowing eljárásra az ENSZ működése során is sor került: James Wasserstrom 65.000 USD összeget ítélt meg az illetékes bíróság, miután retorziók érték, mert koszovói munkájával kapcsolatban korrupciós gyakorlatokat fedett fel.[5]

Míg Magyarországon csak most került elfogadásra egy egységes, átfogó jogszabály a whistleblowing rendszerek működéséről, Angliában a vonatkozó jogszabály (Public Interest Disclosure Act

[3] **SEC settles with whistleblower-employee for $580K** http://newenglandinhouse.com/2013/09/02/sec-settles-with-whistleblower-employee-for-580k/
[4] **Michael Woodford ... the Olympus whistleblower's back in focus** http://www.standard.co.uk/business/markets/michael-woodford--the-olympus-whistleblowers-back-in-focus-8652256.html
[5] **Tribunal orders United Nations to pay $65,000 to whistleblower** http://www.reuters.com/article/2013/03/20/us-un-kosovo-whistleblower-idUSBRE92J1EY20130320

1998) 2013. nyarán már módosították (Enterprise and Regulatory Reform Act 2013) a whisleblowing eljárásokkal kapcsolatos gyakorlati tapasztalatok alapján (szigorítva például a munkáltató felelősségét, ha egy másik munkavállaló hátrányos intézkedést tesz egy whistleblower ellen). Emellett a UK Whistleblowing Commission nevű független szervezet 2013. novemberében közzétett jelentésében 25 további ajánlást tett a munkáltatóknak[6] a whistleblowing rendszerek megfelelő működésével kapcsolatban – javasolta például a rendszerek időszakos auditját, és a tapasztalatok éves beszámolókban való közzétételét. Az EU-s adatvédelmi hatóságok közül legutóbb Dániában bocsátott ki a hatóság állásfoglalást a pénzügyi szektorban üzemeltetett whistleblowing rendszerek által felvetett specifikus kérdésekkel kapcsolatban (Dániában whistleblowing bejelentést nemcsak a munkáltató által létrehozott szervhez, hanem a pénzügyi felügyelő hatósághoz is lehet tenni)[7].

## II. Adatvédelmi és munkajogi aggályok az EU-ban

A fenti trendekkel összhangban a nemzetközi vállalatok whistleblowing rendszereiket globális szinten is bevezették – a személyes adatok kezelése a bejelentési csatornák használata során azonban számos EU országban adatvédelmi aggályokat vetett fel. A whistleblowing rendszereket üzemeltető vállalatok kettős elvárással találták szembe magukat: a rendszer bevezetésével egyrészt meg kellett felelniük az amerikai számviteli- és antikorrupciós szabályoknak, másrészt be kell tartaniuk az EU-s adatvédelmi szabályokat – az adatvédelmi megfelelőség biztosítása viszont sokszor akadálya a whistleblowing rendszerben történő szabad adattovábbításnak.

Franciaországban például az illetékes adatvédelmi hatóság (Commission Nationale de l'Informatique et des Libertés - CNIL) például nem engedélyezte sem a McDonald's France, sem a Compagnie Européenne d'Accumulateurs (CEAC) whistleblowing-rendszerének helyi bevezetését, ugyanis a névtelen bejelentő-vonalak a hatóság álláspontja szerint sértették volna a bejelentésben érintett személyek magánszférájának védelmét.[8] A CNIL véleménye szerint a névtelen bejelentések lehetővé tétele növeli a rosszhiszemű bejelentések kockázatát, és a bejelentések által érintett személyek számára nem biztosított az EU Adatvédelmi Irányelve (a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv) alapján biztosított jog,

[6] http://www.pcaw.org.uk/files/WBC%20Report%20Final.pdf
[7] http://www.datatilsynet.dk/english/whistleblower-systems/whistleblower-guidelines
[8] Részletes összefoglaló a problémáról: **Whistleblowing and Codes of Conduct in Europe – The difficult implementation of SOX whistleblower provisions in France** http://apps.americanbar.org/labor/lel-aba-annual/papers/2006/10.pdf

miszerint információt kérhetnek a személyes adataik kezelésével kapcsolatban (például hozzáférés a névtelen bejelentések alapján készült anyagokhoz, esetleg annak érdekében, hogy megfelelően védekezhessenek a vádak ellen). A hatóság azt is megállapította, hogy az adatkezelési cél – gazdasági bűncselekmények megelőzése – az érintett személyek magánszféráját kevésbé korlátozó módon is elérhető, például a belső eljárások fejlesztésével, vagy a munkavállalók oktatásával, és a rendszerekben kezelt adatok köre sem volt arányos az elérendő céllal. Felmerült kérdésként az is, hogy az érintett franciaországi leányvállalatok az EU-s Adatvédelmi Irányelv hatálya alá tartozó „adatkezelőnek" minősülnek-e egyáltalán – a hatóság szerint igen, pedig a whistleblowing bejelentés közvetlenül az amerikai anyacéghez érkezik, a francia leányvállalat csak ezt követően kaphatja meg az adatokat, közvetlenül az USA-ból.

Hasonlóan járt a Dassault Systèmes nevű szoftvercég is, ahol az illetékes bíróság megállapította, hogy a CNIL által engedélyezett adatkezelésnél szélesebb körben kezeltek adatokat az általuk használt whistleblowing rendszerrel kapcsolatban.[9]

Az orvostechnikai eszközöket gyártó Stryker-cégcsoport franciaországi leánycége, a Benoist Girard számára ugyancsak a SOX alapján volt kötelező a whistleblowing rendszer bevezetése. A leányvállalat előzetesen konzultált az üzemi tanáccsal, észrevételeiket azonban nem építette be a rendszer működésébe, majd amikor módosított a rendszeren, már nem is konzultált az üzemi tanáccsal. A rendszert a CNIL jóváhagyta, az üzemi tanács egészségügyi és biztonsági csoportja azonban bíróságon támadta meg annak bevezetését. Az illetékes bíróság az üzemi tanácsnak adott igazat: a francia jogszabályok értelmében ugyanis az egészségügyi és munkabiztonsági követelményeket érintő döntések előtt kötelező a konzultáció az üzemi tanáccsal, és a whistleblowing rendszer bevezetése és használati feltételeinek megváltoztatása hatással van a munkavállalók közérzetére – vagyis egészségére, és emellett a foglalkoztatói szervezet működésével kapcsolatos általános konzultációs kötelezettség alá is esik. Az illetékes bíróság bírálta továbbá a rendszer kiterjedt hatályát, valamint azt, hogy nem utasítja el automatikusan a nem a rendszer hatálya alá tartozó panaszokat (az ilyen panaszokat továbbító személyek értesítésével). A bíróság megállapította továbbá, hogy az érintett személyeket nem tájékoztatták megfelelően személyes adataikkal kapcsolatos jogaikról és jogorvoslati lehetőségükről, valamint a rendszer használatával kapcsolatos lényeges adatvédelmi feltételekről.

[9] http://www.theworldlawgroup.com/files/file/docs/Soulier%20-%20France%20CNIL%20.pdf

Szintén az üzemi tanáccsal való konzultáció hiánya miatt bizonyult jogellenesnek a Wal-Mart amerikai áruházlánc whistleblowing rendszerének németországi bevezetése. Ebben az esetben az illetékes bíróság magát a whistleblowing eljárás alapját jelentő etikai kódex jogszerűségét is vizsgálta, és megállapította, hogy sérti a munkatársak személyhez fűződő jogait az a rendelkezés, amely megtiltotta a szerelmi kapcsolatot olyan munkavállalók között, akiknek befolyása lehetett egymás munkakörülményeire.[10]

A magyar adatvédelmi hatóság – a korábbi Adatvédelmi Biztos – először 2007-ben foglalkozott a whistleblowing rendszerek által felvetett jogi kérdésekkel, és eleinte meglehetősen kritikusan viszonyult az amerikai gyakorlat európai megvalósításához. Egyik első állásfoglalásában egyenesen kijelentette: „*a panaszbejelentő rendszer… általában szépen hangzó elnevezés ellenére lényegében nem más, mint egy, a munkáltató által működtetett belső besúgó-rendszer*", ami „*hazánkban alapvető fontosságúnak tartott alkotmányos alapjogot és elvet csorbító módszer*", és „*idegen azonban az európai kultúrától*".[11] Az Adatvédelmi Biztos főként történelmi okokból idegenkedett a whistleblowing rendszerek hazai bevezetésétől: véleménye szerint Magyarországon mint az egykori szocialista blokkhoz tartozó államban, sokakban visszatetszést, rossz emlékeket kelt a módszer, ami potenciális besúgóvá teheti a munkatársakat. Azt azonban maga az Adatvédelmi Biztos is elismerte vonatkozó állásfoglalásaiban, hogy a whistleblowing rendszerek magyarországi bevezetését nem tiltja konkrét jogszabály – a munkáltatóknak arra kellett csak figyelniük, hogy megfeleljenek az adatvédelmi jogszabályok rendelkezéseinek, és az Adatvédelmi Biztos kapcsolódó állásfoglalásainak.

Létezik továbbá egy nagyon fontos, egységes európai iránymutatás is: az Európai Bizottság mellett működő független európai adatvédelmi tanácsadó szerv, a 29-es Munkacsoport 2006. február 1-jén bocsátotta ki 1/2006 sz. véleményét az uniós adatvédelmi szabályoknak a számvitel, belső számviteli ellenőrzés, könyvvizsgálati kérdések, korrupció, banki és pénzügyi bűnözés elleni küzdelem terén létrehozott belső visszaélés-jelentési rendszerekre történő alkalmazásáról (a továbbiakban a „**29-es Munkacsoport Véleménye**"). Az Adatvédelmi Biztos kapcsolódó állásfoglalásai is hivatkoznak erre a dokumentumra – tekintettel arra, hogy az Adatvédelmi Biztos jogutódja, a Nemzeti Adatvédelmi és Információszabadság Hatóság egyelőre nem bocsátott ki iránymutatást a whistleblowing rendszerek

[10] **Whistleblowing in Germany** http://www.whistleblower-net.de/pdf/WB_in_Germany.pdf
[11] A legismertebb ügyek, állásfoglalások számai: 271/K/2007-3, ABI-2997-3/2010/P, 295/K/2007-3, 652/K/2007-3.

használatával kapcsolatban, a Whistleblowing Törvény mellett a jogi megfelelőség vizsgálata során a 29-es Munkacsoport Véleménye is irányadó lehet.

### III. A magyarországi Whistleblowing Törvény, és annak legfontosabb rendelkezései

Magyarországon az új, 2014. január 1-től hatályos Whistleblowing Törvény a magánszektor-béli munkáltatók számára az alábbi főbb kötelezettségeket határozza meg (ha pedig a whistleblowing rendszer használata során Magyarország területén is történik adatkezelés / adatfeldolgozás, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény („**Infotv.**") - is irányadó lesz):

#### 1. Nyilvánosságra hozatali kötelezettség

A Whistleblowing Törvény a whistleblowing rendszer használatára vonatkozó eljárási szabályokkal kapcsolatban a következő nyilvánosságra hozatali kötelezettségeket határozza meg:

- A munkáltató szervezet, valamint annak gazdasági társasági formában működő tulajdonosa (a Whistleblowing Törvény szerint együtt: „foglalkoztatói szervezet") a foglalkoztatói szervezet munkavállalóira a munka törvénykönyvéről szóló 2012. évi I. törvény („Munka Törvénykönyve") 9. § (2) bekezdésében meghatározott feltételekkel a közérdeket vagy nyomós magánérdeket védő magatartási szabályokat állapíthat meg, amelyet a foglalkoztatói szervezet a kapcsolódó eljárás leírásával együtt bárki számára elérhető módon köteles nyilvánosságra hozni.[12]

- A foglalkoztatói szervezet a jogszabályok, valamint fenti magatartási szabályok megsértésének bejelentésére visszaélés-bejelentési rendszert (a Whistleblowing Törvény szerint: „bejelentési rendszer" - a jelen írásban a gyakorlatban jobban elterjedt nevén, „whistleblowing rendszerként" is emlegetjük) hozhat létre, ebben a bejelentőnek, valamint a bejelentésben érintett személynek a bejelentésben megadott személyes adatait a bejelentés kivizsgálása céljából kezelheti.[13] A bejelentési rendszer működésére, valamint a bejelentéssel kapcsolatos

[12] Whistleblowing Törvény, 13. §
[13] Whistleblowing Törvény, 14. § (1)

eljárásra vonatkozóan a foglalkoztatói szervezet honlapján magyar nyelvű, részletes tájékoztatást tesz közzé.[14]

A whistleblowing rendszer használata részletes szabályainak közzététele jogszerű elvárás – de csak a foglalkoztatói szervezet működési körén belül! Kérdéses emiatt, hogy a gyakorlatban mennyire ésszerű a fent idézett két nyilvánosságra hozatali kötelezettség. Mind a magatartási szabályok, mind a whistleblowing rendszer működésére vonatkozó szabályok tartalmazhatnak ugyanis olyan, a foglalkoztatói szervezet belső működésére vonatkozó bizalmas információkat, amiknek a nyilvánosságra hozatala sértené az üzleti titkok védelmét, és hátráltatná a whistleblowing eljárás során lefolytatandó vizsgálatok hatékonyságát. A fenti rendelkezések alapján a foglalkoztatói szervezet nehéz helyzetbe kerül: olyan magatartási szabályokat és eljárásrendet kell készítenie, ami megosztható a nyilvánossággal, de mégis megfelelő és hatékonyan végrehajtható, a szervezet tevékenységével összefüggő specifikus szabályokat is tartalmaz. (A Whistleblowing Törvény ugyanakkor nem definiálja, milyen „honlapon" kell teljesíteni a közzétételi kötelezettséget – felmerül a kérdés, hogy adott esetben elég lehet erre egy intranetes honlap, ahol „külsős" személyek nem ismerhetik meg az eljárásrendet?)

### 2. Bejelentkezési kötelezettség az Adatvédelmi Nyilvántartásba

Pozitív fejlemény, és segíti a whistleblowing rendszerekkel kapcsolatos adatkezelések átláthatóságát, hogy a kapcsolódó adatkezelést kötelező bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) által vezetett adatvédelmi nyilvántartásba.[15] A regisztráció korábban csak az Adatvédelmi Biztos ajánlásaként létezett, és ennek alapján sok cég döntött úgy, hogy „a hatóság radarja alatt" marad, és inkább nem jelentették be a whistleblowing rendszerük üzemeltetését – az ajánlást betartó cégek pedig paradox módon „rejtőzködő" társaikhoz képest emiatt jobban ki voltak téve egy-egy hatósági vizsgálatnak. A gyakorlatban a bejelentkezési kötelezettség azt is jelenti, hogy a whistleblowing rendszerek üzemeltetésének elindítása tulajdonképpen a NAIH előzetes jóváhagyásához kötött. A Whistleblowing Törvény nem említi, de ez a kötelezettség vélhetően kiterjed a jogszabály hatályba lépése előtt elindított, akkor még kötelező bejelentési kötelezettség alá nem tartozó rendszerekre is.

[14] Whistleblowing Törvény, 14. § (2)
[15] Whistleblowing Törvény, 14. § (1)

A bejelentési kötelezettség tényleges használatával kapcsolatban persze kérdés, hogy a NAIH az Adatvédelmi Nyilvántartásba való bejelentkezés során kitöltött, általános kérdéseket tartalmazó formanyomtatványokban mennyire tudja felmérni egy komplex adatkezelési célokkal, széles adatkörrel és adattovábbítási lehetőségekkel működő whistleblowing rendszer adatvédelmi megfelelőségét. A hatóságnak vélhetően nincs elég erőforrása ezt esetről-esetre vizsgálni; a bejelentkezési kötelezettség így ugyanakkor egyszerű nyilvántartási, adminisztratív feladattá válik, jelentősebb gyakorlati funkció nélkül. (Dániában például az alkalmazott adatbiztonsági intézkedéseket is be kell jelenteni az adatvédelmi hatóság számára, hogy az nagyobb rálátással rendelkezzen a vonatkozó személyes adatok biztonságos kezelésére.)

### 3. Jogszabály által lehetővé tett adattovábbítások

Szintén pozitív, és gyakorlatias rendelkezés, hogy a Whistleblowing Törvény automatikusan engedélyezi a bejelentés során kezelt személyes adatok továbbítását a bejelentés kivizsgálásában közreműködő külső szervezet részére. Ilyen szervezet például az érintett cég külsős ügyvédje, könyvvizsgálója, valamint az ügy kivizsgálásában közreműködő egyéb szakértő (pl. *forensics*).[16]

A bejelentő személyes adatai a bejelentés alapján kezdeményezett eljárás lefolytatására hatáskörrel rendelkező szerv részére szintén átadhatóak - ha e szerv annak kezelésére törvény alapján jogosult, vagy az adatai továbbításához a bejelentő egyértelműen hozzájárult.[17]

Nem definiálja ugyanakkor a Whistleblowing Törvény, hogy itt csak a magyar jogszabályokra, magyar szervekre gondol, vagy egy nemzetközi szintű cégcsoport esetében külföldi, de extraterritoriális hatályú jogszabályok (pl. FCPA, UK Bribery Act) alapján illetékességgel rendelkező szervek is ideértendők. Erre a bizonytalanságra figyelemmel célszerű lehet szükség szerint a fenti, külföldi szervek részére való adattovábbításra való felhatalmazást a vonatkozó whistleblowing eljárási szabályzatban rögzíteni. A hozzájárulás alapján történő, a Whistleblowing Törvényben külön nem engedélyezett adattovábbítással

[16] Whistleblowing Törvény, 14. § (1)
[17] Whistleblowing Törvény, 3. § (3)

kapcsolatban ugyanakkor – munkaviszony keretében történő, alá-fölérendeltetési viszonyról lévén szó – további kérdés a hozzájárulás valódi „önkéntes" jellege, amit esetről esetre kell elbírálni.

**4. Különleges adatok kezelésének tilalma**

A Whistleblowing Törvény rögzíti, hogy a bejelentési rendszerben különleges adatok kezelése tilos. (Különleges adat: (a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, (b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.)[18] Ha mégis ilyen adatok kerülnek be a whistleblowing rendszerbe, törlésükről (a bejelentés kivizsgálásához nem szükséges adatok törlésével együtt) a foglalkoztatói szervezet kell, hogy gondoskodjon.[19]

A 29-es Munkacsoport Véleménye ugyanakkor ilyen korlátozást nem tartalmaz, és az Adatvédelmi Biztos korábbi ajánlásai sem rendelkeztek így – véleményünk szerint ez az adatkezelési korlátozás rendkívül ésszerűtlen, hiszen számos esetben szükség lehet különleges adatokra az adott visszaélés kivizsgálásához. Jelentős információ lehet például az érintett személy büntetett előélete (bűnügyi személyes adat), de az is elkerülhetetlen lehet, hogy faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre vonatkozó személyes adat (munkahelyi diszkrimináció kivizsgálása esetén) vagy szexuális életre vonatkozó személyes adat (ha a panasz zaklatás kivizsgálására irányul) kerüljön a whistleblowing rendszerbe. Nem beszélve arról, hogy egyes esetekben az érintett személy érdek-képviseleti szervezeti tagsága is fontos eleme lehet az ügynek. Az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat pedig adott esetben szükséges lehet az érintett személy motivációinak felmérésében.

**5. A megvádolható / bejelentő személyek köre**

A Whistleblowing Törvény nem korlátozza sem a jelentésre jogosult személyek, sem a megvádolható személyek körét. Csak a 29-es Munkacsoport Véleménye tartalmaz ezzel kapcsolatban

[18] Infotv. 3. § 3. pont
[19] Whistleblowing Törvény, 14. § (4)

ajánlást, miszerint: „*a visszaélés-jelentési rendszerért felelős vállalat alaposan vizsgálja meg, helyénvaló lenne-e a feltételezett szabálytalanságok visszaélés-jelentési rendszeren keresztül történő jelentésére jogosult személyek számának korlátozása*", valamint „*azon személyek számának korlátozása, akikről a visszaélés-jelentési rendszeren keresztül jelentés készíthető*", „*különös tekintettel a jelentendő feltételezett szabálytalanságok súlyosságára*." [20] A gyakorlatban ugyanakkor ez az ajánlás kevésbé életszerű, hiszen nehezen korlátozható előre a szabályellenes cselekményeket elkövető, illetve ezen cselekményekről tudomást szerző és azokat bejelentő személyek lehetséges köre. Az utóbbiakkal kapcsolatban szerencsére a Whistleblowing Törvény széles körű, gyakorlatias felhatalmazást biztosít: „*A bejelentési rendszerbe a foglalkoztatói szervezet munkavállalói, valamint a foglalkoztatói szervezettel szerződéses viszonyban álló, vagy olyan személyek tehetnek bejelentést, akiknek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdekük fűződik.*" [21] (Svédországban például a megvádolható személyek köre csak a kulcsfontosságú munkavállalókra / menedzsment-tagokra terjed ki – egyéb személyek bűnügyi személyes adatait ugyanis kizárólag állami szervek kezelhetik. Hasonló személyi korlátozás létezik Dániában és Ausztriában is, sőt, az utóbbi országban csak SOX-al kapcsolatos szabályszegéseket jelenthetnek be a munkavállalók.)

**6. Névtelen bejelentések**

A Whistleblowing Törvény nem tiltja kifejezetten a névtelen bejelentéseket, ugyanakkor rendelkezéseivel egyértelműen a nevesített és bizalmasan kezelt jelentéseket támogatja.

A jogszabály ezzel kapcsolatban a következő kötelezettségeket rögzíti a rendszer üzemeltetője számára:

- „*Azonosíthatatlan bejelentő által megtett bejelentés vizsgálata mellőzhető.*"[22]

- „*A bejelentés megtételekor a bejelentő nevét és lakcímét, jogi személy bejelentő esetén annak székhelyét és a bejelentést benyújtó törvényes képviselőjének nevét köteles megadni, továbbá nyilatkoznia kell arról, hogy a bejelentést jóhiszeműen teszi olyan*

[20] A 29-es Munkacsoport Véleménye, IV. pont 2. i)
[21] Whistleblowing Törvény, 14. § (6)
[22] Whistleblowing Törvény, 14. § (6)

*körülményekről, amelyekről tudomása van, vagy kellő alappal feltételezi, hogy azok valósak. A bejelentő figyelmét fel kell hívni a rosszhiszemű bejelentés következményeire, a bejelentés kivizsgálására irányadó eljárási szabályokra és arra, hogy személyazonosságát a vizsgálat valamennyi szakaszában bizalmasan kezelik. A bejelentőt tájékoztatni kell arról, hogy a név nélküli vagy azonosíthatatlan bejelentő által megtett bejelentés vizsgálata mellőzhető.*"[23]

- „*A bejelentési rendszert úgy kell kialakítani, hogy a nem névtelen bejelentő személyét a bejelentést kivizsgálókon kívül más ne ismerhesse meg. A bejelentést kivizsgálók a vizsgálat lezárásáig vagy a kivizsgálás eredményeképpen történő formális felelősségre vonás kezdeményezéséig a bejelentés tartalmára és a bejelentésben érintett személyekre vonatkozó információkat kötelesek titokban tartani, és azokat - a bejelentésben érintett személy tájékoztatása kivételével - nem oszthatják meg a foglalkoztatói szervezet egyetlen más szervezeti egységével vagy munkatársával sem.*"[24]

A fenti, valamint a következő pontban ismertetésre kerülő tájékoztatási kötelezettségek megfelelően átveszik az Adatvédelmi Biztos ezzel kapcsolatos ajánlásait. A korábbi, ajánlási szinten de mégis kvázi kötelező jelleggel bíró szabályozói gyakorlat beépítése a jogszabályba rendkívül pozitív megoldás, és erősíti a jogbiztonságot, a joggyakorlat egységesítését – látszik, hogy a Whistleblowing Törvény alkotói ebben a tekintetben komolyan megvizsgálták a hatályos magyarországi gyakorlatot. Sajnos kimaradt viszont a Whistleblowing Törvényből az Adatvédelmi Biztos azon ajánlása[25], miszerint a rendszer használóit arról is tájékoztatni kell, hogy semmiféle szankcióval sem kell számolniuk a rendszer jóhiszemű használata esetén, pedig egy ilyen tájékoztatás erősítheti a munkaszervezeten belüli bizalmat, különös tekintettel a whistleblowing rendszer használatával kapcsolatos esetleges aggályokra. (A Whistleblowing Törvény általános hiányossága, hogy nem tartalmaz megfelelően részletes előírásokat a jóhiszemű bejelentő védelmével kapcsolatban.)

A bejelentő adatainak bizalmas kezelése alapvető elvárás, és összhangban van a nemzetközi gyakorlattal – érdemes lett volna azonban a titoktartási kötelezettségeket a jogszabályban jobban

[23] Whistleblowing Törvény, 14. § (6)
[24] Whistleblowing Törvény, 15. § (2)
[25] 652/K/2007-3. számú ügy (2007. május 18.)

részletezni; a bejelentő adatain kívül például a lehetséges tanúk, egyéb érintettek adatainak, valamint a vizsgálattal kapcsolatos tényeknek a bizalmas kezelését is fontos lehet kifejezetten előírni.

Gyakorlati szempontból azt is érdemes azonban figyelembe venni, hogy nem lehet 100%-osan biztosítani a bejelentő adatainak bizalmas kezelését: az eljárás egy későbbi szakaszában, például ha az ügyben hivatalos, bírósági eljárás indul, a hivatalos eljárás során a bejelentő személyazonosságára fény derülhet. A 29-es Munkacsoport Véleménye szerint erre is fel kell hívni a bejelentő figyelmét – a Whistleblowing Törvényből azonban ez a megoldás hiányzik.[26]

**7. Általános tájékoztatási kötelezettségek**

A Whistleblowing Törvény a bejelentő, valamint a bejelentésben érintett személy tájékoztatásával kapcsolatban a következőket rögzíti:

*„A bejelentést a foglalkoztatói szervezet köteles kivizsgálni és a bejelentőt a kivizsgálás eredményéről, valamint a megtett intézkedésekről tájékoztatni."*[27]

*„A bejelentésben érintett személyt a vizsgálat megkezdésekor részletesen tájékoztatni kell a rá vonatkozó bejelentésről, az Infotv. alapján megillető jogairól, valamint az adatai kezelésére vonatkozó szabályokról. A tisztességes eljárás követelményének megfelelően biztosítani kell, hogy a bejelentésben érintett a bejelentéssel kapcsolatos álláspontját akár jogi képviselője útján is kifejtse, és azt bizonyítékokkal támassza alá. A bejelentésben érintett személy tájékoztatására kivételesen, indokolt esetben később is sor kerülhet, ha az azonnali tájékoztatás meghiúsítaná a bejelentés kivizsgálását."*[28]

Nem definiálja ugyanakkor a jogszabály, hogy ki minősül pontosan a „bejelentésben érintett személy" – kizárólag a megvádolt személy, vagy azok a harmadik személyek is, akiknek a neve az üggyel kapcsolatban még felmerül (pl. egyéb kollégák, tanúk), de csak a bejelentés teljessége érdekében – a bejelentő egyébként nem vádolja őket szabályellenességgel. Komolyabb hiányossága továbbá a

[26] A 29-es Munkacsoport Véleménye, IV. pont 2. iii)
[27] Whistleblowing Törvény 15. § (1)
[28] Whistleblowing Törvény 15. § (3)

Whistleblowing Törvénynek, hogy a 29-es Munkacsoport Véleményével ellentétben nem rögzíti alapelvi szinten: a megvádolt személy semmilyen körülmények között nem juthat a bejelentő személyazonosságára vonatkozó információhoz a rendszerből a megvádolt személy hozzáférési joga alapján, kivéve, ha a visszaélést jelentő személy rosszhiszeműen hamis kijelentést tesz.[29] (A 9. § pontban van egy erre vonatkozó utalás, de nem egyértelmű a jogszabály szerkezetéből, hogy ez vonatkozik-e a munkahelyi whistleblowing rendszerekre is.)

Egyes EU-s országokban vannak egészen specifikus tájékoztatási kötelezettségek is: Spanyolországban például értesíteni kell a szakszervezetet, ha valamely tagja ellen eljárás indult.

**8. Mellőzhető bejelentések**

A Whistleblowing Törvény szerint lehetővé teszi bizonyos bejelentések mellőzését, az alábbiak szerint:[30]

- „*A korábbival azonos tartalmú, ugyanazon bejelentő által tett ismételt, a sérelmezett tevékenységről vagy mulasztásról való tudomásszerzéstől számított hat hónap után bejelentett, továbbá a név nélküli vagy azonosíthatatlan bejelentő által megtett bejelentés vizsgálata mellőzhető.*"

- „*Ha a közérdek vagy a nyomós magánérdek sérelme a bejelentésben érintett személy jogainak korlátozásával nem áll arányban, a foglalkoztatói szervezet a bejelentés vizsgálatát mellőzheti.*"

Véleményünk szerint a hat hónapos, „kvázi jogvesztő" határidő (még ha végső soron a foglalkoztatói szervezet jogosult eldönteni, él-e az általa biztosított mellőzési lehetőséggel) gyakorlati szempontból indokolatlan, és gátolja az átláthatóság érvényesülését – a whistleblowing rendszerek által „célzott" bűncselekmények (pl. vesztegetés) sokszor hosszabb idő után derülnek ki.

[29] A 29-es Munkacsoport Véleménye, IV. pont 4. ii)
[30] Whistleblowing Törvény 15. § (1)

**9. Adattovábbítás külföldre**

A Whistleblowing Törvény szerint *„az adatok külföldre történő továbbítására akkor kerülhet sor, ha az adatkezelő vagy adatfeldolgozó szerződés keretében kötelezettséget vállal a bejelentésre vonatkozó magyar törvényi szabályok betartására és a továbbított vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére feldolgozásra átadott személyes adatok megfelelő szintű védelme az Infotv. 8. § (2) bekezdése szerint biztosított.”*[31]

Ez a rendelkezés vélhetően az összes külföldi adattovábbításra vonatkozik – bár szerkezetileg nem szerencsés, hogy közvetlenül a bejelentővédelmi ügyvéd megbízására[32] vonatkozó mondat után következik. Az adattovábbítás további garanciákhoz kötése szigorúbb, mint az Infotv. vonatkozó szabályai, és szövege alapján minden külföldi adattovábbítás esetén kötelező – akkor is, ha például az érintett személy önkéntes hozzájárulásán alapul. (Az EU-n kívüli adattovábbítással kapcsolatos fenntartásai nem csak a magyar jogalkotónak vannak. Belgiumban például csak kiemelt esetekben lehetséges egy adott whistleblowing bejelentéssel kapcsolatos adatokat az EU-n kívülre továbbítani – a „helyi” ügyekkel összefüggő személyes adatokat nem. A holland adatvédelmi hatóság iránymutatása pedig kizárólag a menedzsment-szintű jogsértésekkel kapcsolatos személyes adatok EU-n kívüli továbbítását ajánlja.)

Nem szerencsés megoldás, hogy a Whistleblowing Törvény kapcsolódik is az Infotv.-hez, meg nem is, folytatva ezzel (például a biztosítási törvényhez hasonlóan) az adatvédelmi fogalmak nem egységes használatával kapcsolatos jogalkotási anomáliát. A Whistleblowing Törvény esetében a probléma a következő: a „külföld” fogalmát az Infotv. nem ismeri, a Whistleblowing Törvény alkotója viszont vélhetően „külföld” alatt az Infotv. szerinti „harmadik országokat” érti, vagyis minden olyan államot, amely nem EGT-állam. A Whistleblowing Törvény így nem egy, korábban már megfelelően, jogszabályi szinten definiált fogalomra építkezik, átveszi viszont az Infotv. „hírhedt” 8. § (2) bekezdését, ami ebben az összefüggésben a következő követelményét jelenti: a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosítani kell a személyes adatok megfelelő szintű

[31] Whistleblowing Törvény 16. § (1)
[32] A bejelentővédelmi ügyvéd szerepe a jelen írásnak nem tárgya; az ezzel kapcsolatos kérdéseket részletesen a **Pesti Ügyvéd** 2013. októberi cikke tekinti át (**Bizalmi ügyvéd – Átvehető-e a német minta?**)

védelmét, és ez akkor biztosított, ha az EU kötelező jogi aktusa azt megállapítja. Az „EU kötelező jogi aktusának" fogalmát azonban az Infotv. sem definiálja. Véleményünk szerint – és figyelembe véve a NAIH legutolsó adatvédelmi állásfoglalását[33] - „megfelelőnek" kell tekinteni az adatvédelem feltételeit egy harmadik országban, ha az adattovábbításban érintett felek pl. EC Model Clause-t alkalmaznak - abban az esetben is, ha maga az érintett állam nem rendelkezik EU-s szintű adatvédelmi jogszabállyal. Az EC Model Clause elvileg nem jogszabály, ugyanakkor az Infotv. alapján egy, az EU Bizottság által hivatalosan jóváhagyott jogi aktusnak tekinthető. Ugyanez a helyzet a „Safe Harbor" elveknek megfelelő, USA-beli címzett részére történő adattovábbítással is, de az Infotv.-hez hasonlóan a Whistleblowing Törvény sem tartalmaz sajnos utalást a „Kötelező Erejű Vállalati Szabályokra" (*Binding Corporate Rules for International Data Transfers* – *„BCR"*) mint „megfelelő védelmet" biztosító eszközre. A BCR-ok ugyan csak a cégcsoportokon belüli adatcserékre vonatkoznak, de egy whistleblowing rendszerrel kapcsolatos adatcserében ez is elengedhetetlen lehet. A 29-es Munkacsoport Véleménye is kifejezetten nevesíti a BCR-okat[34], tekintettel arra, hogy például ha a jelentés másik csoporttársaság üzletfelét, vagy másik csoporttársaság munkavállalóját érinti – ebben az esetben a BCR lehetne a leghatékonyabb megoldás a „megfelelő védelem" biztosítására.

Az sem teljesen tisztázott, hogy szükséges-e a Whistleblowing Törvény által előírt többlet-garanciák alkalmazása a harmadik országba történő adattovábbítás esetén, ha az adattovábbítást esetleg más jogszabály garanciák nélkül lehetővé teszi – például a társasági törvény a vezető tisztségviselőkkel kapcsolatos adatok harmadik országbeli tulajdonosok részére való továbbítását.

**10. Kivizsgálási határidő**

A Whistleblowing Törvény a kivizsgálási határidővel kapcsolatban a következők szerint rendelkezik:

*„A foglalkoztatói szervezet a körülmények által lehetővé tett legrövidebb időn belül köteles a bejelentésben foglaltak kivizsgálására. A bejelentés kivizsgálására annak beérkezésétől számított 30 nap áll rendelkezésre, amely határidőtől - név nélküli vagy azonosíthatatlan bejelentő által megtett*

[33] http://naih.hu/files/2223-2-2013-v.pdf
[34] A 29-es Munkacsoport Véleménye, IV. pont 7.

*bejelentés kivételével - csak különösen indokolt esetben, a bejelentő egyidejű tájékoztatása mellett lehet eltérni. A vizsgálat időtartama a 3 hónapot nem haladhatja meg.*"[35]

A 3 hónapos időtartam véleményünk szerint a gyakorlatban túl kevés lehet – figyelembe véve a whistleblowing rendszereken keresztül bejelentett egyes szabályszegések összetettségét (pl. számvitelre, számviteli belső ellenőrzésre vagy könyvvizsgálati kérdésekre vonatkozó panaszok). A Whistleblowing Törvény ebben a tekintetben több mozgásteret biztosíthatott volna.

### 11. Feljelentési kötelezettség?

A Whistleblowing Törvény szerint „*ha a bejelentésben foglalt magatartás miatt a vizsgálat alapján büntetőeljárás kezdeményezése indokolt, akkor intézkedni kell a feljelentés megtételéről*." Ezt a rendelkezést többen „feljelentési kötelezettségként" értelmezik – véleményünk szerint azonban a szöveg úgy is olvasható, hogy a foglalkoztatói szervezet saját maga lehet jogosult eldönteni, „indokolt"-e a büntetőeljárás kezdeményezése (vagy az ügy megfelelően és hatékonyabban megoldható „házon belül", például sikkasztás esetén az elkövető számára megfelelő büntetés lehet a jogosulatlanul megszerzett előny visszafizetése és munkajogi szankciók). Egy, a jogszabály által előírt feljelentési kötelezettség csökkentené a whistleblowing során érintett személyek együttműködési készségét, és nem lennének motiváltak a tényállás teljes feltárásában – hiszen végül úgyis büntetőeljárást kellene kezdeményezni ellenük. A fenti szabály „feljelentési kötelezettségként" való értelmezése azt a negatív megközelítést erősítheti, miszerint bizonyos esetekben nem elég az önszabályozás (vagyis, hogy adott esetben a munkáltató a saját belső szervezete keretében, súlyosabb szankciók nélkül helyre tud hozni egy jogsértést, és az állami szervek bevonása szükségtelen és/vagy veszélyeztetné a jogsértés hatékony felderítését és megoldását). Ezt az álláspontunk szerinti rossz megközelítést tartalmazta a korábbi Adatvédelmi Biztos vonatkozó véleménye is, ami a munkáltató érdekét „vélt érdekeknek" tekintette, mert véleménye szerint „fölöttébb valószínű, hogy a rendszer semmilyen kézzelfogható eredménnyel nem fog szolgálni, csak negatív hatásai lesznek.[36] A whistleblowing rendszerek használatával kapcsolatos gyakorlati tapasztalatok ma már azt mutatják, hogy ez egyáltalán nem így van.

[35] Whistleblowing Törvény, 16. § (3)
[36] Ügyszám: 271/K/2007-3

Más a helyzet a rosszhiszemű bejelentőkkel: a Whistleblowing Törvény szövege szerint „*ha nyilvánvalóvá vált, hogy a bejelentő rosszhiszeműen, döntő jelentőségű valótlan információt közölt és (a) ezzel bűncselekmény vagy szabálysértés elkövetésére utaló körülmény merül fel, személyes adatait az eljárás lefolytatására jogosult szerv vagy személy részére át kell adni, (b) alappal valószínűsíthető, hogy másnak jogellenes kárt vagy egyéb jogsérelmet okozott, személyes adatait az eljárás kezdeményezésére, illetve lefolytatására jogosult szervnek vagy személynek kérelmére át kell adni.*”[37] A jogszabály itt már nem biztosít diszkrecionális jogkört a foglalkoztató szervezet számára – ugyanakkor ennek az adatátadási kötelezettségnek a hatékonysága is kérdéses lehet a gyakorlatban.

### 12. Adatmegőrzési és adattörlési kötelezettség

A Whistleblowing Törvény a whistleblowing rendszerek használatával kapcsolatban az alábbi adatmegőrzési és adattörlési kötelezettségekről rendelkezik:

- „*Ha a vizsgálat alapján intézkedés megtételére kerül sor - ideértve a bejelentő személlyel szemben jogi eljárás vagy fegyelmi intézkedés megtétele miatti intézkedést is - a bejelentésre vonatkozó adatokat a foglalkoztatói szervezeti bejelentési rendszerben legfeljebb a bejelentés alapján indított eljárások jogerős lezárásáig lehet kezelni.*”[38]

- „*Ha a vizsgálat alapján a bejelentés nem megalapozott vagy további intézkedés megtétele nem szükséges, a bejelentésre vonatkozó adatokat a vizsgálat befejezését követő 60 napon belül törölni kell.*”[39]

A 29-es Munkacsoport Véleményében szereplő általános, és kevésbé gyakorlatias szabály („*a vonatkozó személyes adatokat általában a jelentésben állított tények vizsgálatának befejezését követő két hónapon belül törölni kell*”)[40] a Whistleblowing Törvényben szerencsére nem szerepel. Kérdés persze, hogy a gyakorlatban mit takar a „bejelentésre vonatkozó adatok” fogalma – egy-egy fegyelmi, bírósági vagy egyéb hatósági eljárással összefüggő, jogszerűen keletkezett személyes adatokat (és az azokat tartalmazó hivatalos iratokat) indokolt lehet megőrizni belső archiválási vagy compliance célból,

[37] Whistleblowing Törvény, 14. § (5)
[38] Whistleblowing Törvény 16. § (5)
[39] Whistleblowing Törvény 16. § (6)
[40] A 29-es Munkacsoport Véleménye, IV. pont 2. v)

továbbá esetleges további igények (pl. polgári peres igények) felmérése céljából. Ilyen esetekben a Whistleblowing Törvény által rögzített adattörlési kötelezettség kevésbé indokolt és életszerű.

Felmerül annak is a lehetősége, hogy egy eredménytelen vizsgálat esetén a megvádolt személy jogi lépéseket tesz a bejelentő személy vagy a foglalkoztató szervet ellen – ebben az esetben az adattörlési kötelezettség miatt a megtámadott személyek számára nem állnak rendelkezésre a vonatkozó adatok a megfelelő védekezéshez. Az adott esettől függően megfontolható lehet az adatok jogszerű megőrzésének biztosítására az Infotv. 6. § (1) bekezdését alkalmazni, miszerint „*személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.*”

## 13. Egyéb szabályok

A Whistleblowing Törvényben kifejezetten rögzített rendelkezéseken túl egy whistleblowing rendszer üzemeltetésekor meg kell felelni mind az általános munkajogi, mind az adatvédelmi jogszabályoknak, melyek a következők:

### 13.1 Konzultáció az üzemi tanáccsal

A Munka Törvénykönyvének 264. § (1) pontja szerint „*a munkáltató döntése előtt legalább tizenöt nappal kikéri az üzemi tanács véleményét a munkavállalók nagyobb csoportját érintő munkáltatói intézkedések és szabályzatok tervezetéről.*” Ilyen munkáltatói intézkedésnek minősül különösen a munkavállalóra vonatkozó személyes adatok kezelése és védelme és a munkavállaló ellenőrzésére szolgáló technikai eszköz alkalmazása. Az idézett szabályok értelmében a whistleblowing rendszer – és nagy valószínűséggel az alapjául szolgáló magatartási szabályok – bevezetése előtt Magyarországon konzultálni kell az üzemi tanáccsal. Mivel az Munka Törvénykönyve a vonatkozó munkáltatói intézkedések között nem nevesíti a whistleblowing rendszerekkel kapcsolatos magatartási

szabályok és eljárásrend bevezetését, célszerű lett volna ezt az esetleges eltérő jogértelmezések elkerülése végett a Whistleblowing Törvényben rögzíteni.

### 13.2 Adatkezelés alapelvek

Az Infotv. 4. § szerint:

- Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető.
- Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának; az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.
- Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas.
- A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
- Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

A Whistleblowing Törvény által engedélyezett adatkezelési célt – „*közérdeket vagy nyomós magánérdeket védő magatartási szabályok megsértésének bejelentése*" – tehát ezekkel az alapelvekkel összhangban kell értelmezni. Adatvédelmi szempontból ugyanakkor komoly hiányossága a Whistleblowing Törvénynek, hogy nem specifikálja jobban az engedélyezett adatkezelési célt, például a 29-es Munkacsoport Véleményéhez hasonlóan. Az utóbbi értelmében a whistleblowing rendszerek használata során engedélyezett adatkezelési cél a számvitelre, számviteli belső ellenőrzésre vagy könyvvizsgálati kérdésekre vonatkozó panaszok, csalás és a kötelességszegés megelőzése, korrupció, banki és pénzügyi bűnözés vagy a bennfentes kereskedelem elleni küzdelem.[41] A gyakorlatban visszatérő kérdés, hogy használható-e a rendszer emberi jogok sérelmének kivizsgálására (például munkahelyi zaklatás), vagy egyéb jogellenes cselekmények (például biztonságos munkavégzés követelményeinek, szellemi alkotások és üzleti titkok védelmének, összeférhetetlenségi szabályoknak vagy környezetvédelmi kötelezettségek megszegése) felderítésére. A korábbi jogszabály legalább az indokolásában tett ennek szabályozására egy

[41] A 29-es Munkacsoport Véleménye, IV. pont 2. iv)

óvatos kísérletet, tágan és gyakorlatiasan határozva meg az érintett magatartásformákat; a Whistleblowing Törvény sajnos nem rendelkezik ilyenről, így célszerű a részletes adatkezelési célokat a vonatkozó belső eljárási szabályzatban meghatározni.

### 13.3 Adatvédelmi tájékoztatási kötelezettségek

A whistleblowing rendszer működésével kapcsolatban irányadó belső szabályzatnak tartalmaznia kell az érintett személyek számára az általános adatvédelmi információkat is a rendszerben kezelt adatokkal kapcsolatban. Az Infotv. ezzel összefüggésben előírja, hogy az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő az Infotv. 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.[42] Az adatvédelmi tájékoztató elkészítésekor figyelemmel kell lenni a NAIH mindenkori ajánlásaira is – például az EGT-n kívüli harmadik országokba való adattovábbításokkal kapcsolatos további tájékoztatási kötelezettségekre.

### 13.4 Adatbiztonsági követelmények

A whistleblowing rendszer üzemeltetésekor a foglalkoztatói szervezetnek figyelembe kell vennie az Infotv. 7. § által meghatározott általános adatbiztonsági szempontokat is:

- „*A rendszerben kezelt adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.*”
- „*A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt*

[42] Infotv. 20. §

*adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.*" (Különösen fontos lehet ez a whistleblowing rendszerek működtetésével kapcsolatban, mert a vizsgálattal kapcsolatban több, párhuzamos HR adatbázis létrehozatala is szükséges lehet.)

- „*Az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.*"

A fentiek persze csak általános követelmények – az adott IT intézkedést a foglalkoztatói szervezet maga kell, hogy meghatározza, figyelemmel az adott iparág mindenkori „legjobb gyakorlatára".

A 29-es Munkacsoport Véleménye szerint a vállalaton vagy vállalatcsoporton belül különálló szervezetet kell létrehozni a visszaélésekről szóló jelentések kezelésére és a vizsgálatok vezetésére. E szervezetnek korlátozott számú, speciálisan képzett és erre kijelölt személyzetből kell állnia, akiket különleges titoktartási kötelezettségek szerződésben köteleznek. E visszaélés-jelentő rendszert szigorúan el kell különíteni a vállalat más részlegeitől, mint például a humán erőforrás osztály.[43]

### 13.5 Az érintettek jogai és jogorvoslati lehetőségei

Az Infotv. által biztosított jogok és jogorvoslati lehetőségek keretében a whistleblowing rendszer működésével kapcsolatban érintett személy kérelmezheti az adatkezelőnél (vagyis általában a foglalkoztatói szervezetnél) tájékoztatását személyes adatai kezeléséről, személyes adatainak helyesbítését, valamint személyes adatainak - a kötelező adatkezelés kivételével - törlését vagy zárolását.[44] Ezzel kapcsolatban fontos, hogy az érintett kérései teljesítése során az adatkezelő a Whistleblowing Törvény specifikus szabályaira is figyelemmel legyen (pl. a bejelentő adatainak bizalmas kezelése), valamint az se váljon lehetővé az érintett személy számára, hogy visszaélésszerűen, a jogszerű vizsgálat akadályozása céljából töröltesse személyes adatait a rendszerből. Az adott esettől függően

[43] A 29-es Munkacsoport Véleménye, IV. pont 6. i)
[44] Infotv. 20. §

ebben az esetben is megfontolható lehet az Infotv. 6. § (1) már említett bekezdését alkalmazni, miszerint *„személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.”* Az Adatvédelmi Biztos korábbi állásfoglalásaiban szintén megállapította[45], hogy az adatkezeléssel kapcsolatos jogok gyakorlása korlátozott a rendszer által érintett más személyek jogai és szabadságai védelmének biztosítása érdekében, és e korlátozást eseti alapon kell alkalmazni.

**IV. „Házi feladat”**

A Whistleblowing Törvénynek való megfelelés biztosítása érdekében a cégeknek – a fenti szabályok figyelembevételével – a következőket kell tenniük a meglévő, illetve a jövőben bevezetésre kerülő whistleblowing eljárásrendjeikkel kapcsolatban:

1. A vonatkozó magatartási szabályok, etikai kódexek, belső eljárási szabályok és specifikus whistleblowing-szabályok azonosítása.

2. Ellenőrizni, hogy a fenti dokumentumok megfelelnek-e a Whistleblowing Törvény eljárási szabályainak (pl. határidők, tájékoztatási kötelezettségek) és adatvédelmi előírásainak (pl. a rendszerben kezelhető adatok köre). Ha valamely globális belső szabály ellentétes az új jogszabállyal, érdemes lehet külön magyarországi kiegészítést készíteni.

3. A vonatkozó eljárási szabályok megfelelő közzététele és az érintett személyek tájékoztatása.

4. Ellenőrizni, hogy a whistleblowing rendszerrel kapcsolatban sor kerül-e adattovábbításra az EU-n kívülre; ha igen, akkor milyen intézkedésekkel biztosítják az adatok megfelelő védelmét (pl. Safe Harbor, EC Model Clauses).

[45] 652/K/2007-3. számú ügy (2007. május 18.)

5. A whistleblowing rendszer üzemeltetésével kapcsolatban megkötésre került szolgáltatási szerződések (pl. IT szolgáltatók, egyéb szakértők, adatfeldolgozók) vizsgálata a jogszabályi megfelelőség szempontjából (különös tekintettel az adatbiztonsági elemekre).

6. A whistleblowing rendszer bejelentése az Adatvédelmi Nyilvántartásba, a meglévő bejelentés(ek) folyamatos aktualizálása.

7. Konzultáció az üzemi tanáccsal, ha szükséges.

8. Oktatás és megfelelő titoktartási kötelezettségek bevezetése a whistleblowing rendszer megfelelő használatával kapcsolatban (külön a munkavállalók, és külön a rendszer üzemeltetésében részt vevő személyek számára).

A Whistleblowing Törvénynek való megfelelés már csak azért is fontos, mert az a munkáltató, aki a rendszert üzemelteti, felelősséggel tartozik a jogellenes adatkezelésért. Hátrányos jogkövetkezmény lehet a NAIH által adatvédelmi bírság (mértéke százezertől tízmillió forintig terjedhet), sőt, a NAIH elrendelheti határozatának - az adatkezelő azonosító adatainak közzétételével történő - nyilvánosságra hozatalát, ha azt az adatvédelem érdekeinek, illetve nagyobb számú érintett jogainak védelme megköveteli. A Whistleblowing Törvény megsértése esetén felmerülhet továbbá a jogszabálysértő személy polgári jogi felelőssége (az érintett személyek személyhez fűződő jogainak sérelme), valamint súlyosabb esetben bűncselekmény (pl. személyes adattal visszaélés, levéltitok megsértése, becsületsértés, rágalmazás).

*A szerző ügyvéd, a CMS Cameron McKenna LLP budapesti irodájának munkatársa, számos alkalommal nyújtott tanácsot whistleblowing eljárási szabályzatok készítése, lokalizációja és gyakorlati alkalmazása során. Az írással kapcsolatos kérdéseket, észrevételeket a marton.domokos@cms-cmck.com vagy a marton.domokos@gmail.com címre várja.*