A DPO SZEREPE AZ ADATVÉDELMI ÖNELLENŐRZÉSBEN, AZ ÖNELLENŐRZÉS SZEREPE AZ ADATVÉDELMI MEGFELELÉSBEN

SZERZŐ: DR. CSEKŐ KATALIN - ADATVÉDELMI TISZTVISELŐ: AUCHAN MAGYARORSZÁG KFT, MH AUCHAN BENZINKUTAK KFT., FŐTITKÁR: MAGYAR ADATVÉDELMI TUDATOSSÁGÉRT TÁRSASÁG EGYESÜLETE

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (a továbbiakban: GDPR) 39. cikk (1) bekezdésének b) pontja[1] az adatvédelmi tisztviselő feladatai közé sorolja az ellenőrzésekben való részvételt. Mégis azt olvashatjuk a Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolóiban, hogy a DPO-k fele nem vesz részt ellenőrzési/audittervek kidolgozásában, vagy ellenőrzések/auditok elvégzésében.[2]
Az ellenőrzésre időt szánni az alapelveknek megfelelő működés egyik kulcseszköze lehet, így adatvédelmi tisztviselőként,ha eddig nem vettünk részt belső ellenőrzésben a klasszikus értelemben vett adatvédelmi auditban, érdemes ezen változtatnunk és minden lehetséges ellenőrzési szintben megtalálni a szerepünket.

Az adatkezelőnél végezhető ellenőrzések három szinten valósíthatóak meg:

1. az adatvédelmi önellenőrzés, melyet az adatkezelő terület végez
2. adatvédelmi ellenőrzés, melyet nem az adatkezelő terület, hanem vagy az adatvédelmi terület, vagy egy szakmai szempontú ellenőrzést végző más szervezeti egység végez; az ellenőrzésen túl magában foglalja az egyes szintű önellenőrzés vizsgálatát, ami az önellenőrzés megtörténtének rendszerességéről, minőségéről és megfelelőségéről ad információt
3. adatvédelmi audit az adatkezelőnél vagy adatfeldolgozóinál az adatkezelő audit részlege vagy külső auditor által, ahol adott esetben a DPO mint szakértő támogatja az auditorok munkáját.

Jelen cikkben nem a klasszikus, az ellenőrzés 3. szintjét jelentő adatvédelmi audittal, hanem az 1-2. típusú belső ellenőrzési folyamatokkal foglalkozunk.

[1] Az adatvédelmi tisztviselő ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;
[2] A NAIH 2021-es és 2020-as beszámolói alapján 2020-ban a DPOK-k 42,8%-a, 2021-ben 47,2%-a készített belső ellenőrzési (audit) tervet; 2020-ban 40,5%, 2021-ben 44,8% folytatott dokumentált módon belső ellenőrzést (auditot)

Biztosan sokan ismerik az ikonikus mondást: „Nem lehet minden pofon mellé egy forgalmi rendőrt állítani”.[3] Ez az adatkezelő szervezetének működtetésére is igaz, pláne a nagyszámú adatkezelést végző szervezeti egységgel rendelkező adatkezelőknél. A DPO bármennyire is szeretné, fizikailag lehetetlen, hogy folyamatosan mindenhol személyesen vizsgálja az adatvédelmi megfelelést, így szüksége lesz olyan kulcsemberekre, akik ezt rendszeresen megteszik, majd megosztják vele az ellenőrzések eredményét, ő pedig levonhatja belőle a következtetéseket.

Ha az adatvédelmi tisztviselő megtalálta a kulcsembereit, nem dőlhet hátra azt követően hogy az adatkezelő illetékes területével karöltve végigviszi az önellenőrzési feladat és felelősség szervezési intézkedésbe (szabályzat, munkaköri leírás) foglalását. Mivel az önellenőrzést végző területek a folyamatokat még az oktatások ellenére is elsősorban szakmai és nem adatvédelmi szemmel nézik, a DPO segítségére és szakértelmére van szükség önellenőrző listák kialakításához, melynek köszönhetően már a terület kezében lesz az önellenőrzés elvégzésének kulcsa. Gyakorlati tapasztalatom, hogy nem elég leírni, hogy mit ellenőrizzenek, de szükséges a jó megoldás ismérveit is felsorolni: pl. ha ellenőrizni kell, hogy az adatkezelési tájékoztató aktuális-e, akkor rendszeresíteni kell egy olyan felületet, ahol az összes aktuális anyag megtalálható, de még ennél is jobb megjelölni a tájékoztató legújabb részét, melynek alapján néhány másodperc alatt kiderül az ellenőrzést végző számára, hogy az általa látott anyag aktuális-e.

Az adatvédelmi tisztviselő az önellenőrzésekből kapott visszajelzések alapján fogja látni, hogy a követelmények, amelyeket támasztott a munkatársak felé, számukra érthetőek és valóban illeszkednek-e a munkafolyamatokhoz. Ha a hiányosságok folyamatosan fennállnak vagy ismétlődnek, annak csak az egyik lehetséges oka a munkatársak hanyagsága. Több olyan ok is lehet, ami a DPO-n is múlik: tudatosítás, megfelelő feladatmeghatározás hiánya, illetve az adatvédelmi követelmények folyamatidegensége. Az önellenőrzések kiértékelésekor tehát nem az az egyetlen következmény, hogy a mulasztók felelősségre vonását kezdeményezze a vezetőknél az adatvédelmi tisztviselő, hanem célszerű párbeszédet indítania a szakmai és az adatkezelési követelmények jobb összhangja érdekében.

A belső fejlődésből leginkább az olyan területeken lehet látványosan profitálni, ahol az adatkezelés a kirakatban, az érintettek szeme előtt zajlik, és ekképpen különösen alkalmas arra, hogy az érintett akár az adatkezelőhöz benyújtott panaszt,érintetti kérelmet kihagyva,

[3] Rejtő Jenő: Piszkos Fred, a kapitány

a hatósághoz forduljon. A személyesen, helyben nyújtott, adatkezeléssel járó szolgáltatások, vevőszolgálatok üzemeltetése pl. tipikusan ilyen eset. Hétköznapi hibák vezethetnek hatósági ügyekhez: hiába készül el a világ legtökéletesebb adatkezelési tájékoztatója, ha annak nem a legfrissebb, az adatkezelést ténylegesen leíró változata kerül az érintett elé. Ha nem ellenőrizzük rendszeresen, hogy incidensmegelőző intézkedéseink működnek-e sokkal nagyobb eséllyel bekövetkezik a baj: pl. a kereskedelemről szóló 2005. évi CLXIV. törvény 5.§ (4a) bekezdése alapján a vásárlók könyvéből haladéktalanul ki kell tépni a bejegyzést tartalmazó lapokat[4]. Napi szintű önellenőrzés nélkül az adatvédelmi incidensnek hatalmas az esélye, ha ezt a rendelkezést nem tartják be. Ugyanígy hiába készültek remek fotók a honlapra, ha azoknak az adatvédelmi hátterét nem rendezték.

A DPO által végzett ellenőrzés

A szakmai irányító területek ellenőrzése, holott már egy magasabb szintű ellenőrzés, a DPO szempontjából és a módszereket illetően megegyezik az önellenőrzésekkel, így jelen pontban kizárólag a DPO ellenőrzéseit tekintjük át.

Az adatvédelem és művelői még mindig gyakran részesülnek abban a negatív megítélésben, hogy elefántcsonttoronyból szónokolnak. A DPO által végzett ellenőrzés az egyik legjobb módja annak, hogy erre rácáfoljon. Ez természetesen csak akkor valósul meg, ha túl tud lépni az adatbekéréssel végzett ellenőrzéseken és visszatérő jelleggel helyszíni ellenőrzésre, helyszínbejárásra is sort kerít. Sok telephely esetén persze nem fog mindenhova eljutni egy év alatt, de ezekből a látogatásokból is számos következtetés levonható.

A módszer (beszélgetés, iratbetekintés, helyszínbejárás, próbavásárlás) ezekben az esetekben teljes mértékben rajta múlik. Ami biztos, hogy érdemes az ilyen látogatások során nyitott szemmel járni, mert ez a legjobb alkalom arra, hogy láthassa, valóban minden folyamatba be lett-e vonva, vagy szembejön vele olyasmi, amiről nem tudott, így adatvédelmi szempontból kockázatot jelent az érintettekre és az adatkezelőre is. Az önellenőrzéshez képest itt mindenképpen plusz tényező a szakmai szem. Számos, látszólag bárki számára észlelhető hibát lehet így észrevenni, pl. azonnal kiszűrhető, ha az adatkezelési tájékoztatót úgy készítik el helyben, hogy az az átlagember számára nem látható helyen van vagy olvashatatlan.

[4] Más vásárlók által a vásárlók könyvébe bejegyzett személyes adatok megismerése lehetőségének kizárása céljából a vásárlók könyvéből a kereskedő a bejegyzést követően haladéktalanul eltávolítja a (4) bekezdés szerint panaszt vagy javaslatot tartalmazó oldalt, azt elzártan - a folyamatos sorszámozás rendjének megfelelően - megőrzi és a hatóság felszólítására rendelkezésre bocsátja

Lehet, hogy akad, aki úgy gondolja, hogy ezek elengedhető szempontok, de ha felidézzük pl. a Vodafone bírságot[5], ahol az ügy azért indult, mert „a bejelentő továbbá arról számolt be, hogy a „számhúzó rendszer" második „választós képernyőjén" lehet látni a többihez képest kevésbé feltűnő betűkkel és helyen elhelyezve egy tájékoztatást", máris látható, hogy szükség van a szakértői szemre a „terepen".

A helyszínen a hibákon túl felfigyelhetünk a megváltozott körülményekre, amelyre reagálni kell, pl. megszűnt adatkezelési célokhoz tartozó dokumentáció eltávolítása, helyiség funkciójának megváltozása - kamerás adatkezelések kapcsán.

Ezen az ellenőrzési szinten a DPO-nak feladata az is, hogy az általa végzett ellenőrzés eredményét összevesse az önellenőrzések eredményével, így könnyen kiszűrhető, ha a területi kulcsember nem adott meg valós adatot, nem vagy nem megfelelően végezte az ellenőrzést vagy egy hiba, hiányosság visszatérő jellegű az adott területen vagy ugyanaz a hiba több telephelyen, szervezeti egységnél is fennáll.

Ezeknek az ellenőrzéseknek ugyanúgy megvan az a haszna, mint az önellenőrzésnek: csökkenti az adatkezelőnél jelentkező kockázatokat, a bírságnak való kitettséget, de ezen túl is hatalmas profitot jelent a DPO számára: folyamatosan tanulhat újat az adatkezelő szervezetéről, naprakész lehet, kétoldalú kommunikációt alakíthat ki az adatkezelő területekkel, reagálhat a problémáikra, ezzel együtt emészthetőbbé teheti számukra az adatvédelmi elvárásokat, megalapozhatja a területek bizalmát, ezzel pedig azt, hogy ha éppen nincs a helyszínen, akkor is bevonják a folyamatok kialakításába.

Ezek az ellenőrzések tehát olyan eszközök, amelyek támogatják az adatkezelő adatvédelmi megfelelését, egyben pedig jobb szakemberré tesznek minket. Éljünk velük!

[5] NAIH/2020/2758/4. számú határozattal kiszabott 60 millió Ft-os bírság