

**Szakmai szempontok
az adatvédelmi audit végzéséhez**



Tartalomjegyzék

| | |
|------------------------------------------------------------------------------------------------------------|-----------|
| AZ ADATVÉDELMI AUDIT | 3 |
| AZ ADATVÉDELMI AUDIT ELŐNYEI | 4 |
| AZ ADATVÉDELMI AUDIT CÉLJA | 5 |
| AZ ADATVÉDELMI AUDIT MÓDSZERTANA | 6 |
| AZ ADATVÉDELMI AUDIT MENETE | 10 |
| AZ ADATVÉDELMI AUDIT ÉRTÉKELÉSE | 13 |
| JELENTÉS NYILVÁNOSSÁGA | 15 |
| TITOKTARTÁS, ÖSSZEFÉRHETETLENSÉG, AZ ADATVÉDELMI AUDIT ÉS A HATÓSÁG EGYÉB ELJÁRÁSAINAK VISZONYA | 15 |
| AZ ADATVÉDELMI AUDIT ELLENÉRTÉKE | 16 |
| JOGSZABÁLYI HÁTTÉR | 17 |



Az adatvédelmi audit

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) értelmében az adatvédelmi audit a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) olyan szolgáltatása, amelynek célja a végzett vagy tervezett adatkezelési műveletek a Hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása. Ennek megfelelően a Hatóság az alábbi szempontrendszerben kívánja megismertetni az adatvédelmi audit intézményét az érintettekkel.

Az adatvédelmi audit az adatkezelő kérelmére indul. Az adatvédelmi audit mind a magánszféra, mind a közszféra számára hatékony segítséget jelent abban, hogy az adatkezeléseiket szakértő áttekintse, és gyakorlati tanácsokkal segítse az adatvédelmi előírásoknak való minél teljesebb megfelelést. A Hatóság által megfogalmazott ajánlások várhatóan elősegítik az információs önrendelkezési jog hatékonyabb érvényesülését.

Az audit a számvitel és a minőségellenőrzés területén meghonosult eljárás, amelyet azóta számos egyéb szektorokban is használnak. Az audit lényegében egy vizsgálatot jelent, amely egy rendszerre, tevékenységre, eljárásra, folyamatra vonatkozik. Célja, hogy megvizsgálja, az adott rendszer, eljárás mennyire felel meg az előírásoknak, elvárásoknak, szabványoknak. Az audit mára egy általános, felülvizsgálati eszköz lett, amely alapján független harmadik szereplők értékelik az auditált szervezet eljárásait.

Az auditnak több fajtája alakult ki, amelyek többféle szempont szerint csoportosíthatóak. Megkülönböztethetünk belső vagy külső auditot, illetve alkalmassági vagy megfeleléségi auditot. Belső audit esetén a szervezet maga vizsgálja meg eljárásai megfeleléségét, míg külső audit esetén egy kívülálló személy végzi a felülvizsgálati tevékenységet.



Alkalmassági auditról akkor beszélünk, amikor az auditot végző azt vizsgálja, hogy az adatkezelő dokumentált szabályzatai, adatvédelmi nyilatkozatai, általános szerződési feltételei, gyakorlati útmutatói, munkáltatói iránymutatásai, valamint belső és külső eljárásai összhangban vannak-e a jogszabályi előírásokkal. A megfelelőségi auditnak pedig az a célja, hogy megvizsgálja, az adatkezelő a gyakorlatban ténylegesen a dokumentált szabályzatai, adatvédelmi nyilatkozatai, általános szerződési feltételei, gyakorlati útmutatói, munkáltatói iránymutatásai, belső és külső eljárásai szerint működik. A fentiek alapján tehát az audit egy kontroll mechanizmus függetlenül attól, hogy belső vagy külső auditról, illetve alkalmassági vagy megfelelőségi auditról beszélünk. Bármelyik audit eljárásról is van szó, alapvető követelmény, hogy az auditot végzők rendelkezzenek az adott (jog)területhez szükséges különleges szakértelemmel.

A Hatóság az adatvédelmi audit keretében külső alkalmassági auditot végez.

Az adatvédelmi audit eljárás során a Hatóság felméri, hogy az adatkezelő adatvédelmi ismeretei mennyire naprakészek, illetve az adatvédelmi jogszabályi rendelkezések mennyire tükröződnek belső szabályzataiban. Emellett a Hatóság megvizsgálja, hogy az adatkezelő adatkezeléseivel kapcsolatosan van-e szabályozási hiányosság, felmerülnek-e adatvédelmi kockázatok, illetve megállapítja, milyen lépéseket kell tenni, hogy megvalósuljon a jogszabályoknak megfelelő adatkezelés, valamint ajánlásokat tesz arra nézve, hogy a belső szabályzatok, differenciált szabályozás mentén igazodjanak a szervezet által végzett tevékenységek specialitásaihoz.

Az adatvédelmi audit előnyei

Az adatvédelmi audit előnyei:

- az adatvédelmi auditot kérő adatkezelő jelzi az érintettek felé, hogy fontos számára az adatvédelem és elkötelezett az adatvédelmi előírások betartása iránt;
- megvalósul az adatkezelések független kontrollja;



- az adatkezelő a Hatóság tapasztalt munkatársainak szakértelmére támaszkodva alakíthat ki a jogszabályi előírásoknak megfelelő adatkezelést;
- felmérésre kerülnek az adatvédelmi kockázatokat és az adatkezelő javaslatokat kap a hiányosságok kiküszöbölésére;
- a Hatóság aktívan részt vesz az adatvédelmi előírások nemzetközi szabályozásában, így mindig a legújabb elveket és ismereteket figyelembe véve tudja az adatvédelmi auditot elvégezni;
- az adatkezelő kérelmére indul az eljárás, így az adatkezelő határozhatja meg az adatvédelmi audit célját, terjedelmét.

Az adatvédelmi audit célja

Az adatvédelmi audit célja, hogy az adatkezelő egy független szakértő féllal, a Hatóság közreműködésével felmérje, milyen adatkezeléseket végez, mennyire jártas az adatvédelemben és mennyire felelnek meg szabályzatai az adatvédelmi előírásoknak.

Az adatvédelmi audit során a Hatóság megismeri, az adatkezelő adatkezeléseit, felméri az adatkezelő tudatosságát, illetve megvizsgálja az adatkezelő dokumentált szabályzatait, adatvédelmi nyilatkozatait, általános szerződési feltételeit, gyakorlati útmutatóit, munkáltatói iránymutatásait, belső és külső eljárásait.

Az auditra az adatkezelő számára nyújtott segítségként érdemes tekinteni. Az adatvédelmi auditnak ugyanis az a célja, hogy elősegítse az adatkezelő számára az adatvédelmi előírásoknak történő minél teljesebb megfelelést. Az audit a Hatóság és az adatkezelő kölcsönös együttműködésén alapszik, ennek megfelelően a folyamat során alkalom nyílik arra, hogy az adatkezelő az észrevételeit és elvárásait előadja. Az audit az adatkezelő kérelmére indul, ezért az adatkezelőnek nagy szabadsága van az audit céljának és hatókörének meghatározására.



Az adatvédelmi audit módszertana

A Hatóság három módszert alkalmaz az adatvédelmi audit eljárás során. Egyrésztől kérdőíves lekérdezéssel, másrésztől személyes konzultáció alapján méri fel az érintett adatkezeléseket, illetve az adatkezelő jogtudatosságát, harmadrésztől szakértő munkatársai segítségével elemzi az adatkezelő dokumentált szabályzatait, azok esetleges hiányosságaira és kockázataira összpontosítva.

Az adatvédelmi audit módszertana a külső, alkalmassági audit módszertanához igazodik. Az eljárás során az adatkezelő dokumentált szabályzatainak áttekintése, elemzése és az auditált féllel folytatott konzultáción keresztül a Hatóság az adatkezelő által végzett adatkezelésekről adekvát képet alkot.

Az adatvédelmi audit keretében a Hatóság az adatkezelő által folytatott adatkezeléseket az alábbi szempontok szerint értékeli:

1. A tisztességes adatkezelés elve [Infotv. 4. § (1) bekezdés]. A személyes adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. A személyes adatok védelméhez fűződő jogot sérti az adatkezelés, amennyiben az adatkezelő, bár eljárása formálisan megfelel a vonatkozó törvényi előírásoknak, tisztességtelen módon kezeli a személyes adatokat.

2. A célhoz kötöttség elve [Infotv. 4. § (1) bekezdés]. A célhoz kötöttség elve az adatkezelésre vonatkozó egyik legfontosabb, nemzetközileg kimunkált alapelv, amely értelmében személyes adat kizárólag meghatározott célból kezelhető. A cél csak társadalmilag indokolt, jog gyakorlása vagy kötelezettség teljesítése lehet. Az adatkezelésnek minden szakaszában, így például az adattovábbítás esetén is meg kell



felelnie az adatkezelés céljának. Az adatkezelés célját előre meg kell határozni és közölni az érintettel, aki ily módon megfelelően gyakorolhatja információs önrendelkezési jogát.

3. Az adatminimalizálás elve [Infotv. 4. § (2) bekezdés]. Az adatfelvételbe bevont érintettek körét és a cél eléréséhez szükséges adatfajtákat az adatkezelés célja határozza meg: csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. Ezen alapelv figyelembe vétele szavatolja, hogy az adatkezelés céljára tekintettel csupán a legszűkebb, indokolt adatkör kezelésére kerül sor. Az adatminimalizálás elve továbbá kizárja a készletezésre történő adatkezelést, azaz hogy olyan adatok felvételére kerüljön sor, amelyeket csak később meghatározásra kerülő célból gyűjtenek.

4. Az adatminőség elve [Infotv. 4. § (4) bekezdés]. Az adatok minőségének követelménye is a nemzetközileg kidolgozott alapelvek közé tartozik, amely a tisztességesség és törvényesség kritériumán túl a pontos, teljes és naprakész adatok kezelését teszi az adatkezelő kötelezettségévé. Az adatkezelőnek mindig pontosan rögzítenie kell az érintettől felvett személyes adatokat. Ezen adatoknak teljesnek kell lenniük és az adatkezelés során biztosítani kell naprakészségüket is.

5. A személyes adatot törölni kell, ha az adatkezelés célja megszűnt [Infotv. 17.§ (2) bekezdés]. A célhoz kötöttség elvéből következik az is, hogy amennyiben teljesült az adatkezelés célja, akkor a kezelt személyes adatokat törölni kell. Amennyiben ez nem történne meg, akkor cél nélküli, azaz készletező adatkezelés valósulna meg. Bizonyos jogszabályok külön rendelkezhetnek arról, hogy mely esetekben kell a személyes adatokat az adatkezelési cél megvalósulását követően is kezelni, tárolni.

6. Az érintett jogainak érvényesítése [Infotv. 5-6., 14-21. §]. Személyes adatot – a kötelező adatkezelést kivéve – csak hozzájárulás alapján, vagy az Infotv. 6. §-ában meghatározott külön jogalapok szerint lehet kezelni. Az érintettet még az adatkezelés megkezdése előtt, de ezen felül kérésére bármikor, egyértelműen és részletesen tájékoztatni kell az adatkezeléssel összefüggő minden lényeges körülményről. Az érintett



kérheti adatai helyesbítését, bizonyos esetben törlését is, valamint törvényben meghatározott esetekben tiltakozhat személyes adatai kezelése ellen.

7. Az adatbiztonság [Infotv. 7. §]. Az adatkezelési műveleteket úgy kell megtervezni és végrehajtani, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, továbbá – a technika mindenkori fejlettségére tekintettel – meg kell tennie azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat 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.

8. Adattovábbítás külföldre [Infotv. 8. §]. Személyes adat harmadik országba történő továbbítása megfelel-e a jogszabályi előírásoknak.

A fenti vizsgálat mellett az adatvédelmi audit arra is irányul, hogy a Hatóság megvizsgálja:

- vannak-e az adatvédelmi elvárásokra vonatkozó szabályzatok és eljárások;
- ezek megfelelnek-e az adatvédelmi előírásoknak;
- hol jelennek meg adatvédelmi kockázatok az adott szabályzatokban és eljárásokban;
- milyen ajánlások és jó gyakorlatok ismertek a fenti kockázatok kiküszöbölésére.

Az adatkezelővel folytatott előkészítő tárgyaláson kerül meghatározásra, hogy az adatkezelő mely szabályzatait vizsgálja meg az adatvédelmi audit során. A Hatóság az audit alá vont szabályzatokat mind az általános adatvédelmi elvárások szemszögéből, mind az adott ágazat specifikus előírásainak oldaláról vizsgálja. Az audit alá vont szabályzatok elemzésekor a Hatóság feltárja azok adatvédelmi szempontból aggályos vagy hiányos pontjait és ajánlásokat tesz a kockázatok orvosolására.

Az adatvédelmi audit kockázatelemzésen alapul, a Hatóság megvizsgálja,



- mi a valószínűsége annak, hogy a szabályzatok hiányosságai hatással lesznek az érintettekre;
- milyen hatást gyakorolnak az érintettek az adatkezelő szabályzatainak hiányosságai.

A Hatóság az adatvédelmi kockázatok és az érintettekre gyakorolt hatás elemzésekor az alábbiakat veszi figyelembe:

- az érintettek száma;
- a kezelt személyes adatok jellege;
- az egyes adatkezelési műveletek;
- az adatkezelés célja;
- a szükségesség;
- az arányosság;
- az adatkezelés időtartama;
- az adatok pontossága és teljessége;
- az adatok rendelkezésre állása;
- a megfelelő jogalap megléte;
- adatbiztonsági előírások;
- az érintett jogainak érvényesülése;
- a tájékoztatási kötelezettség érvényesülése.

Összefoglalva elmondható, hogy az adatvédelmi audit során használt módszertan kérdőíves lekérdezésen, személyes konzultáción, a dokumentált szabályzatok elemzésén és jó gyakorlatok propagálásán alapul. Az audit eljárás sikeressége nagymértékben múlik azon, hogy az auditra jelentkező adatkezelő a Hatóság által feltett kérdésekre minél részletesebb választ adjon, illetve dokumentált szabályzatait teljes körben a Hatóság rendelkezésére bocsássa.

Az adatvédelmi audit sikeressége a résztvevő felek együttműködésének a függvénye. Az adatvédelmi auditra jelentkező adatkezelőtől elvárt, hogy a Hatóság munkatársainak a



lehető legteljesebb információkat szolgáltatassák az audit alá vont adatkezelésekkel kapcsolatban.

Az adatvédelmi audit során a Hatóság minden esetben az adott adatkezelő és az audit alá vont adatkezelés sajátosságait figyelembe véve alkalmazza a fenti módszertant. Ennek megfelelően a Hatóság nem használ formalizált kérdőíveket, illetve a személyes konzultáció tematikáját sem kívánja behatárolni. Az eljárás mindig az audit alá vont adatkezelés sajátosságaihoz igazodik. Ez egyben azt is jelenti, hogy az adatvédelmi audit fenti rendszere adatkezelőnként szektor specifikus kérdésekkel egészülhet ki.

Az adatkezelő által folytatott adatkezelések összetettsége esetén az adatvédelmi audit csak az adatkezelő bizonyos adatkezelési műveleteinek, pl. munkavállalókkal vagy ügyfelekkel kapcsolatos adatkezelések áttekintésére is irányulhat.

A Hatóság kizárólag adatvédelmi aspektusból vizsgálja az adatkezeléseket, más jogterületekkel kapcsolatos szabályoknak történő megfelelésről nem tud nyilatkozni, még akkor sem, ha az adatvédelmi audit jelentés során nem csak adatvédelmi szabályozásra hivatkozik.

Az adatvédelmi audit menete

Az adatvédelmi audit eljárás az adatkezelő kérelmére indul. Az adatkezelő határozza meg, mely adatkezelése legyen az audit tárgya. Tervezett adatkezelési műveletek akkor vonhatók audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi.

Az adatvédelmi audit eljárás a hatóság által a honlapján közzétett „Jelentkezés adatvédelmi auditra” című jelentkezési lap kitöltésével kérhető. A jelentkezési lap beérkezését követően a Hatóság egy előzetes, tájékoztató kérdőívet küld az



adatkezelőnek. Az előzetes kérdőív célja az audit alá vont adatkezelések teljesebb megismerése, amennyiben az előzetes kérdőívben szereplő kérdések pontosításra szorulnak, akkor a Hatóság személyesen is felveszi a kapcsolatot az adatkezelővel. Az előzetes megbeszélés továbbá lehetőséget nyújt arra is, hogy minden, az audittal kapcsolatos kérdés tisztázódjon, az audit folyamatát a felek átbeszéljék.

Ha az előzetes kérdések tisztázódtak, akkor a Hatóság megkeresésben tájékoztatja az auditra jelentkező adatkezelőt arról, hogy

- a Hatóság befogadta kérelmét;
- mi az adatvédelmi audit tervezett időpontja;
- mely adatkezeléseket vonják adatvédelmi audit alá;
- mennyi az adatvédelmi audit ellenértéke;
- az adatvédelmi audit menetéről.

Az adatvédelmi audit tervezett időpontját a Hatóság egyezteti az adatkezelővel. A beérkező kérelmek függvényében a Hatóság azonban nem mindig tud személyre szabott időpontot garantálni.

A Hatóság fenntartja a jogot arra, hogy maga határozza meg az adatvédelmi auditok időpontjait és menetrendjét. Az adatvédelmi audit a Hatóság szolgáltatása és nem jog, ennek megfelelően nincs jogi kötelezettség, amely alapján egy adatkezelő valamely adatkezelését a Hatóság köteles adatvédelmi audit alá vonni.

Adatvédelmi auditot a Hatóság az adatkezelő kérelmére folytathat le. Az adatvédelmi audit lefolytatása iránti kérelem benyújtását követő tizenöt napon belül az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét és az adatvédelmi audit elvégzésének várható időpontját a Hatóság közli az adatkezelővel. A Hatóság az adatvédelmi auditot abban az esetben folytatja le, ha a Hatóság közlését követő tizenöt napon belül az adatkezelő nyilatkozik arról, hogy a Hatóság közlésében megállapított feltételek ismeretében az adatvédelmi audit lefolytatása iránti kérelmét fenntartja.



Ha a feltételeket mindkét fél elfogadta, a Hatóság a meghatározott időpontot megelőzően részletes, az adatkezelő adatkezelési műveleteihez igazodó kérdőívet küld az adatkezelő számára, amelynek segítségével áttekinti az adatkezelő adatkezeléseit, az adatkezelő jogtudatosságát, az adatkezelésekkel érintettek számát és egyéb szektor specifikus szempontokat. A Hatóság a kérdőívekkel egyidejűleg bekéri az adatkezelő audit alá vont szabályzatait.

A bekért dokumentumok magukba foglalják különösen az adatkezelő adatkezelési nyilatkozatait, adatkezelési szabályzatait, általános szerződési feltételeit, adatkezelési tájékoztatóit, adatbiztonsági szabályzatait, etikai kódexeit, és minden olyan, az adatkezelő által kiadott írásos dokumentumot, amely személyes adatok kezelését érinti.

A hatóság az audit alá vont dokumentumokról átvételi jegyzőkönyvet vesz fel. A Hatóság az adatvédelmi auditban résztvevő munkatársai az adatkezelő részére titoktartási nyilatkozatot tesznek.

A kérdőívre adott válaszok áttekintése előtt a Hatóság egy előzetes eljárásban felkészül az auditra. A felkészülés során a Hatóság áttekinti,

- az adatkezelőt érintően a hatósághoz érkezett panaszokat;
- az adott szektor számára a Hatóság által kibocsátott jelentősebb állásfoglalásokat;
- az adott szektor számára a Hatóság által kibocsátott ajánlásokat;
- a vonatkozó hazai joggyakorlatot;
- a vonatkozó nemzetközi joggyakorlatot;
- a szektor számára fellelhető jó gyakorlatokat;
- a Hatóság által az adatkezelőt érintő korábbi adatvédelmi audit megállapításait;
- a Hatóság által a hasonló szektorban tevékenykedő adatkezelőket érintő korábbi adatvédelmi audit megállapításait;
- amennyiben az adatkezelő hozzájárul, az adatkezelő által lefolytatott belső audit megállapításait;
- az adatkezelő adatvédelmi nyilvántartásban szereplő bejelentéseit;
- áttekinti az adatkezelő honlapját.



Az adatkezelővel folytatott előzetes megbeszélés, a kérdőívekre adott válaszok és az audit alá vont szabályzatok beérkezését, illetve az előzetes felkészülést követően a Hatóság a fenti módszertan alapján lefolytatja az adatvédelmi auditot.

Az adatvédelmi audit értékelése

Az audit lezárását megelőzően a Hatóság egy záró megbeszélést tart az adatkezelő döntésre jogosult vezetőivel, amelyben áttekinti a felfedezett hiányosságokat, kockázatokat és átbeszéli a lehetséges megoldási lehetőségeket.

A végleges értékelést megelőzően a Hatóság megküldi az előzetes értékelését az adatkezelőnek. Az előzetes értékelésben a Hatóság egy áttekintő összegzést nyújt az audit során megismert adatkezelésekről, elemzi az audit során megismert adatvédelmi kockázatokat és ajánlásokat tesz azok kiküszöbölésére.

Az adatkezelőnek az előzetes jelentés átvételét követően, megfelelő határidő mellett, a Hatóság lehetőséget biztosít a jelentésben megállapított ténybeli tévedések korrigálására, illetve a jelentésben leírt kockázatokkal szemben ellenvéleményének kifejtésére.

A Hatóság az audit jelentés végső megállapításainak megszövegezésében megpróbál egyetértésre jutni az adatkezelővel. Ugyanakkor a Hatóság tudatában van annak, hogy ez nem minden esetben lehetséges. Az adatkezelő válaszát a Hatóság elemzi és megpróbálja ennek tükrében megfogalmazni végső megállapításait. Ugyanakkor a végső audit jelentés tartalmát minden esetben a Hatóság határozza meg.

Az előzetes véleményre adott válasz beérkezését, illetve a válaszadási határidő lejártát követően a Hatóság kibocsátja az adatvédelmi auditról szóló végleges értékelését, amely egy részletes jelentésből és egy vezetői összefoglalóból áll. A jelentés megküldésével egy



időben a Hatóság megfelelő határidő tűzése mellett felhívja az adatkezelőt, hogy nyilatkozzon arról, hozzájárul-e az audit jelentés vezetői összefoglalójának nyilvánosságra hozatalához. Amennyiben az adatkezelő nem tesz erre irányuló nyilatkozatot, akkor az adatvédelmi audit értékelése nem nyilvános.

Az audit jelentés magába foglalja az audit eljárás ismertetését, a megismert adatkezelési folyamatokat, az adatkezelő összes adatkezelésének értékelését az adatvédelmi alapelvek tükrében, az egyes adatkezelési eljárások erősségeit és kockázatait, ajánlásokat, amelyekkel az adatvédelmi előírásoknak történő pontosabb megfelelés elérhető. A végső jelentés egyértelmű ajánlásokat tartalmaz az adatkezelő számára, amelyekkel elősegítheti az adatvédelmi szabályoknak való teljesebb megfelelést. Az audit jelentés nem csak a hiányosságokról, hanem a dokumentumok, az adatkezelő eljárásainak pozitív részeiről, erősségeiről is beszámol.

A végső audit értékelés törekszik az adatkezelő adatkezeléseinek minél szélesebb körű vizsgálatára, ugyanakkor semmilyen vizsgálat sem lehet teljes körű. Az audit eljárás során az adatkezelő valamennyi adatkezelésének áttekintésére nincs lehetőség. Az audit jelentés megállapításai egy adott időpontra vonatkoznak és mindig a kontextus függvényei. A végső jelentés megállapításait az adott időpontban és az adott környezetben kell értelmezni. Egy pozitív kicsengésű értékelés az adatkezelőnek az adatvédelem iránti elkötelezettségét igazolja, valamint azt jelenti, hogy az adott időpontban az adatkezelő szabályzatai megfelelnek az adatvédelmi előírásoknak. Egy pozitív audit értékelés sem mentesíti az adatkezelőt az adatvédelmi szabályok betartása alól, illetve az audit értékelés csak az audit keretében vizsgált adatkezelések tekintetében tanúsítja a megfelelést.



Jelentés nyilvánossága

A jelentés nyilvánosságáról minden esetben az adatkezelő dönt. Ha az adatkezelő hozzájárulását adja, akkor a Hatóság a honlapján az adatvédelmi auditról szóló értékelés vezetői összefoglalóját nyilvánosságra hozza. Ha az adatkezelő az értékelés nyilvánosságra hozatalához nem járul hozzá, akkor a Hatóság a honlapján csupán azt a tényt teszi közzé, hogy az adatkezelést adatvédelmi audit keretében vizsgálta.

Az adatvédelmi audit eredményét rögzítő értékelés tartalma az üzleti titokra alkalmazandó szabályok szerint ismerhető meg.

A fenti rendelkezések nem érintik a közérdekű adatigénylés keretében a Hatósághoz érkező megkeresések teljesítését.

A Hatóság fenntartja a jogot továbbá arra, hogy az audit jelentésben szereplő megállapításokat a Hatóság éves beszámolójában anonim módon szerepeltesse.

Titoktartás, összeférhetlenség, az adatvédelmi audit és a Hatóság egyéb eljárásainak viszonya

A Hatóság az audit eljárásban érintett dokumentumok tekintetében teljes titoktartással tartozik. A Hatóságnak az auditban részt vevő valamennyi munkatársa titoktartási nyilatkozatot köteles aláírni az audit során általa megismert információkat illetően. A titoktartási nyilatkozatok egyik példányát a Hatóság az adatkezelőnek átadja.

A Hatóság az auditot nem bírságot, hanem az adatkezelések megfelelőségét elősegítő eszköznek tekinti. Ha az adatvédelmi audit során jogellenes adatkezelésre derül fény a



Hatóság a végleges értékelés kibocsátása előtt megfelelő határidő tűzésével felszólítja az adatkezelőt a jogellenesség orvoslására. Ha az adatkezelő a Hatóság felszólításának nem tesz eleget, akkor a Hatóság fenntartja a jogot arra, hogy az audit keretein kívüli eszközzel kényszerítse ki a jogellenesség megszüntetését.

Az egész audit folyamatnak, a felkészüléstől az audit értékelés kibocsátásáig, a célja, hogy az adott adatkezelő tudatosabban viszonyuljon az adatvédelemhez. Ebből adódóan az audit a Hatóság figyelemfelkeltő, tudatosságot erősítő, mediáló eszközei közé tartozik és nem bírságot kiterjesztésére szolgál. Ugyanakkor, ha a Hatóság az adatvédelmi audit keretében bűncselekményt észlel, vagy olyan információk jutnak a tudomására, amelyek az adatvédelmi hatósági eljárás megindításának kötelező esetkörébe tartoznak, akkor az adatkezelő értesítése mellett a szükséges intézkedéseket megteszi.

A Hatóságnak az adatvédelmi auditban résztvevő munkatársai a Hatóság által, az adatkezelővel szemben indított adatvédelmi hatósági eljárásában nem vehetnek részt.

Az adatvédelmi auditban nem vehet részt a Hatóságnak azon munkatársa, amely az adatkezelő döntésre jogosult tagjával, képviselőjével a Polgári Törvénykönyvről szóló 1959. évi IV. törvény 685. § b) pontja szerinti hozzátartozója, illetve akitől egyéb okból nem várható el az audit eljárás pártatlan lefolytatása.

Az adatvédelmi audit ellenértéke

Az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét – az elvégzendő tevékenység mértékével arányosan – a Hatóság állapítja meg, az azonban nem haladhatja meg az ötmillió forintot. Az adatvédelmi audit lefolytatásáért fizetendő ellenérték a Hatóság bevétele.



Az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékének meghatározása során a Hatóság különösen az alábbi szempontokat veszi figyelembe:

- az audit alá vont adatkezelések összetettsége;
- az érintettek száma;
- a kezelt személyes adatok jellege;
- az egyes adatkezelési műveletek komplexitása;
- az adatkezelő éves árbevételének mértéke.

Jogsabályi háttér

az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

69. § (1) Az adatvédelmi audit a Hatóság olyan szolgáltatása, amelynek célja a végzett vagy tervezett adatkezelési műveletek a Hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása. Tervezett adatkezelési műveletek akkor vonhatók audit alá, ha az adatkezelésre vonatkozó koncepció kidolgozottsága ezt lehetővé teszi.

(2) Adatvédelmi auditot a Hatóság az adatkezelő kérelmére folytathat le. Az adatvédelmi audit lefolytatása iránti kérelem benyújtását követő tizenöt napon belül az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét és az adatvédelmi audit elvégzésének várható időpontját a Hatóság közli az adatkezelővel. A Hatóság az adatvédelmi auditot abban az esetben folytatja le, ha a Hatóság közlését követő tizenöt napon belül az adatkezelő nyilatkozik arról, hogy a Hatóság közlésében megállapított feltételek ismeretében az adatvédelmi audit lefolytatása iránti kérelmét fenntartja.

(3) Az adatvédelmi audit lefolytatásáért fizetendő ellenérték mértékét – az elvégzendő tevékenység mértékével arányosan – a Hatóság állapítja meg, az azonban nem haladhatja meg az ötmillió forintot. Az adatvédelmi audit lefolytatásáért fizetendő ellenérték a Hatóság bevétele.



(4) Az adatvédelmi audit eredményét a Hatóság az auditról készített értékelésben rögzíti. Az értékelés javaslatokat fogalmazhat meg az adatkezelő számára. Az értékelés tartalma az üzleti titokra alkalmazandó szabályok szerint ismerhet ő meg, az adatkezelő erre irányuló kérelmére azonban a Hatóság honlapján – a kérelemnek megfelelően – az értékelést vagy az értékelés összegző megállapításait közzéteszi.

(5) Az adatvédelmi audit a Hatóság e törvényben rögzített egyéb hatásköreinek gyakorlását nem korlátozza.