Kézikönyv

Célszerű az adatvédelmi közösséggel véleményeztetni mint amely az Infotv-ben – 69.§ (1) – definiált, a Hatóság által meghatározott és közzétett szakmai szempontok szerint készült.

Javasolható továbbá, hogy az audit megkezdése előtt tájékozódjunk a kérelmező szervezet jellemzőiről:

- a szervezet fő tevékenysége,
- alkalmazottainak száma,
- elkülönült adatkezelések szervezeti egységek szerint,
- közülük hányan foglalkoznak adatkezeléssel,
- az adatfeldolgozó – ha van ilyen – megbízásának részletei,
- adattovábbítások címzettjei,
- stb.

Kinek:

- a NAIH auditorainak,
- az adatkezelőnek, aki saját rendszerét teszi vizsgálata tárgyává,
- vállalkozásoknak, melyek audit szolgáltatást nyújtanak.

Az audit során elvégzendő tevékenységek időigénye segíthet az audit igazságszolgáltatási díjának megállapításában.

Minthogy nem idézi fel egyéb törvények adatvédelmi rendelkezéseit, meglehetősen általános. Adott esetben a NAIH szakmai szempontjai sem tartalmazhatnak mást, mint utalást egyéb törvényi rendelkezésekre, melyeknek való megfelelést az audit során vizsgálni fog.

Bevezetés

E kézikönyv összeállításával és közreadásával a NAIH segíteni kívánja az adatvédelmi audit végrehajtását, melynek célja annak ellenőrzése, hogy az adatkezelő adatvédelmi rendszerei megfelelnek az Infotv-ben meghatározott követelményeknek. Az audit új feladat, a korábbi adatvédelmi törvény ilyesmiről nem rendelkezett. Az Infotv szerint a Hatóság nemcsak ellenőrzi, hanem elő is segíti a személyes adatok védelméhez való jog érvényesülését /38. § (2)/. E feladatkörében egyrészt meghatározza az adatvédelmi auditálás szakmai szempontjait, másrészt az adatkezelő kérelmére adatvédelmi auditot folytathat le /38. § (4) g), h)/.

A kézikönyv a módszer ismertetése során útmutatót ad az audit elvégzésére, továbbá ellenőrzőlistákat tartalmaz, melyek kérdéseire adott válaszok értékelésével megállapítható, megfelel-e, s milyen mértékben az adatkezelő a vele szemben támasztott törvényes kötelezettségeknek.

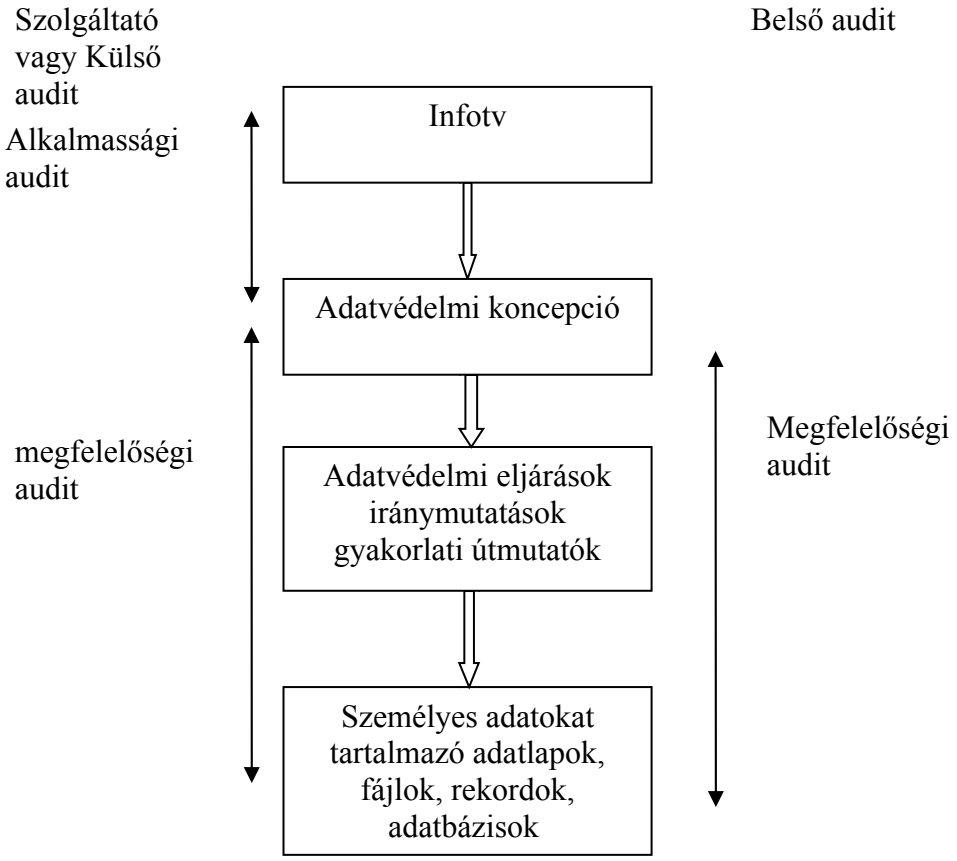
Az audit célja annak megállapítása, hogy az adatkezelő érvényesíti az Infotv-ben tükröződő adatvédelmi alapelveket, éspedig
1. Az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie /4.§ (1)/.
2. Személyes adat kizárólag meghatározott célból kezelhető; az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának /4.§ (1)/.

3. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas /4.§ (2)/.
4. Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és naprakészségét / 4.§ (4)/.
5. A személyes adatot törölni kell, ha az adatkezelés célja megszűnt /17.§ (2)/.
6. A személyes adatok kezelése során biztosítani kell az érintett jogainak érvényesítését /5. és 6.§, 7.§ (1), 20.§, 21.§/.
7. Az adatkezelő megfelelő szervezési és technikai intézkedésekkel köteles gondoskodni az adatok biztonságáról; az adatokat megfelelő intézkedésekkel védenie kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen /7.§/.
8. Személyes adat külföldre csak akkor továbbítható, ha az adatkezelés helyszínéül szolgáló ország a személyes adatok kezelése során biztosítja az érintett jogainak megfelelő szintű védelmét /8.§/.

Az audit fajtái

Audit kategória	Végzi
Belső	A szervezet maga saját magán
Szolgáltató	A szervezet a szállítón vagy az alvállalkozón
Külső	A NAIH, vagy alvállalkozója vagy egy független szakértő a szervezeten

Kissé szemléletesebben:



A belső auditot a szervezet saját magán végzi. Felettébb hasznos, hiszen elvégzésével a szervezetet az adatvédelem proaktív és legjobb gyakorlata kialakítása felé tereli. A belső audit tervszerű, rendszeres végrehajtása és az alkalmazottak továbbképzése növeli a szervezetnek a saját rendszerébe vetett, objektív bizonyítékokon nyugvó bizalmát. Az ismétlődő külső és belső auditok ugyanakkor fokozzák az alkalmazottak adatvédelmi tudatosságának általános színvonalát.

A szolgáltatói audit arra szolgál, hogy a szervezet meggyőződjön arról, hogy a potenciális vagy tényleges szolgáltató vagy alvállalkozó képes teljesíteni az Infotv követelményeit. Mivel manapság általános az a tendencia, hogy a szervezetek mind több és több adatfeldolgozási tevékenységet kiszerveznek, a szolgáltató auditálása egyre fontosabb szerepet játszik az adatfeldolgozó kiválasztásában, majd folyamatos ellenőrzésében. Mindazonáltal a szervezetnek saját magának nem szükséges elvégeznie a szolgáltató auditálását, ha az igazolja, hogy már sikeresen kiállt egy adatvédelmi auditot, feltéve hogy azt egy jó hírű és független harmadik fél végezte.

A külső auditot a szervezettől független személy végzi, éspedig

- a NAIH az adatkezelő kérelmére (Infotv 38/4/h), a Hatóság által meghatározott és közzétett szakmai szempontok szerint (Infotv 69/1),
- külső auditor az adatkezelő megbízásából:

ebben az esetben az adatkezelő arról szándékozik meggyőződni, hogy rendszere megfelel-e az Infotv követelményeinek és a NAIH által meghatározott és közzétett szakmai szempontoknak.

Külső audit – Belső audit

Külső audit		Belső audit
Alkalmassági audit	Infotv	
Megfelelősségi audit	Szabályzatok	Megfelelőségi audit
	Gyakorlati Útmutatók, Iránymutatások és Eljárások	
	Személyes adatokat tartalmazó adatlapok, fájlok, rekordok, adatbázisok	

Az Alkalmassági Audit célja, hogy megvizsgálja, a dokumentált Szabályzatok, Gyakorlati Útmutatók, Iránymutatások és Eljárások teljesítik-e az Infotv-ben rögzített követelményeket. Az auditnak ezt a részét kell először elvégezni. Lényegét tekintve íróasztali munka, amely a helyszíntől függetlenül végezhető. Természetesen lehetséges, hogy az Alkalmassági Auditot belső auditorok hajtják végre, feltéve, hogy rendelkeznek az Infotv követelményeinek értelmezéséhez szükséges különleges szakértelemmel.

A Megfelelőségi Audit célja, hogy megvizsgálja, a szervezet ténylegesen a dokumentált Szabályzatok, Gyakorlati Útmutatók, Iránymutatások és Eljárások szerint működik. Az auditnak ez a leglényegesebb része, s ezt a helyszínen kell elvégezni.

A Belső Audit csak a Megfelelőségi Auditot öleli fel, mert

- Sokkal hatékonyabb annak az adatvédelmi rendszernek a tervezett Belső Auditja, amelyet szabályszerűen dokumentáltak és folyamatosan működik.
- Az adatvédelmi rendszer elvileg teljesíti az Infotv követelményeit, hiszen annak megfelelően kellett megtervezni és megvalósítani.
- Ha az adatvédelmi rendszer már régebb óta megfelelően működik, feltehetően már a megvalósítás folyamán vagy üzemeltetése során tárgya volt egy független harmadik személy által végzett Alkalmassági Auditnak.

Ezért általános gyakorlat, hogy a Belső Audit nem öleli fel az Alkalmassági Auditot. Ez természetesen nem zárja ki, hogy a szervezetek belső audit terveik szerint Alkalmassági Auditot is végezzenek, amely különösen hasznos lehet olyan új rendszerek vagy fejlesztések esetében, amikor külső közreműködőt nem vettek igénybe.

Az audit célja annak megállapítása, hogy	Ezek bizonysága	Alkalmassági audit	Megfelelőségi audit
A rendszer létezik és alkalmas	Dokumentált szabályzatok, útmutatók stb.	Igen	Igen
A rendszert használják	Adatalany hozzáférési	Nem	Igen

	igényének, panaszának stb. rögzítése		
A rendszer működik	Helyesbítés, a rendszer frissítése és fejlesztése	Nem	Igen

A táblázatból egyértelműen kiviláglik az Alkalmassági és a Megfelelőségi Audit közötti különbség:

- az Alkalmassági Audit fő feladata annak igazolása, hogy a dokumentált adatvédelmi rendszer alkalmas az Infotv valamennyi követelményének teljesítésére,
- a megfelelőségi audit arra irányul, hogyan és mily hatékonyan használják az adatvédelmi rendszert.

Az alkalmassági audit

A szolgáltató és a külső audit szempontjából lényeges, hogy először az alkalmassági auditot kell elvégezni, hiszen annak eredményétől függ, mi lesz a következő lépés. Az alkalmassági audit két lehetséges eredménye:

Az alkalmassági audit megfelelő
Ha az alkalmassági audit eredményeképpen megállapítható, hogy dokumentált adatvédelmi rendszer kielégítő, bár esetleg kisebb hiányosságokat mutat, az audit a megfelelőségi audittal folytatható (lásd lentebb).

Az alkalmassági audit nem megfelelő
Az alkalmassági audit során fény derül arra, hogy a szervezet adatvédelmi dokumentációja elégtelen, az eljárások leírása pontatlan és súlyos hiányosságot mutat, például az adatvédelmi tudatosságot fokozó oktatás terén. Ha az auditor ilyen súlyos hiányosságokra bukkant a munkának már ebben az első szakaszában, döntenie kell a folytatás mikéntjéről, melyre ilyen körülmények között három lehetősége adódik:

A szervezet ragaszkodhat a megfelelőségi auditnak a lehetséges megoldások meghatározása elősegítését szolgáló folytatásához, hogy kezelni tudja a rendszereiben már feltárt súlyos hiányosságokat és gyengeségeket.

Az auditor közölheti a szervezettel azt az álláspontját, hogy nincs sok értelme a megfelelőségi audit elvégzésének mindaddig, amíg a súlyos hiányosságokat ki nem küszöbölik.

Az auditor javasolhatja a szervezetnek, hogy adatvédelmi tanácsért vagy útmutatásért forduljon a NAIH-hoz vagy másokhoz annak érdekében, hogy adatvédelmi rendszereik hiányosságait kiküszöbölhessék.

Megfelelőségi audit

A megfelelőségi auditot általában két alapvető módszer szerint végzik, melyek vagy önállóan vagy vegyesen alkalmazhatók.

Funkcionális vagy vertikális audit

Ez az audit a szervezet egy meghatározott – funkcionális vagy szervezeti – egységén belül ellenőrzi az adatvédelmi rendszer valamennyi jellemzőjét. A funkcionális audit a szervezeti egységen belüli folyamatokra, eljárásokra, rekordokra stb. korlátozódik, nem lépi át a szervezeti egységek határait. Az auditornak célszerű az adatvédelmi munkatársaktól tájékoztatást kérni, hiszen ők rendelkeznek a legbehatóbb ismeretekkel arról, hogyan valósítják meg a szervezeti egységek a szervezet átfogó adatvédelmi felfogását.

Példaként említhető egy személyzeti főosztály funkcionális auditja. Ebben az esetben a főosztály funkciójával kapcsolatos személyzeti fájlok, eljárások stb. többnyire a főosztályon belül maradnak, következésképpen az audit a főosztályon belül kezelt személyes adatok felvételével, feldolgozásával stb. kapcsolatos műveletek ellenőrzésére korlátozódhat.

Az ábra egy vertikális, funkcionális egységekre tagozódó szervezet tipikus felépítését szemlélteti. Mindazonáltal meg kell jegyezni, hogy bár a funkcionális audit a személyzeti főosztályra összpontosít, figyelembe kell vennie a szervezet adatvédelmi szabályzatát, a szervezet erőforrásait és rekordjait, amelyek közvetlenül vagy közvetve a személyzeti főosztály funkcióira vonatkoznak.

Adatvédelmi rendszer					
Szervezet					
TERMELÉS	MARKETING	KERESKEDELEM	PÉNZÜGY	SZEMÉLYZETI	ÜGYFÉLSZOLG
Rekordok					

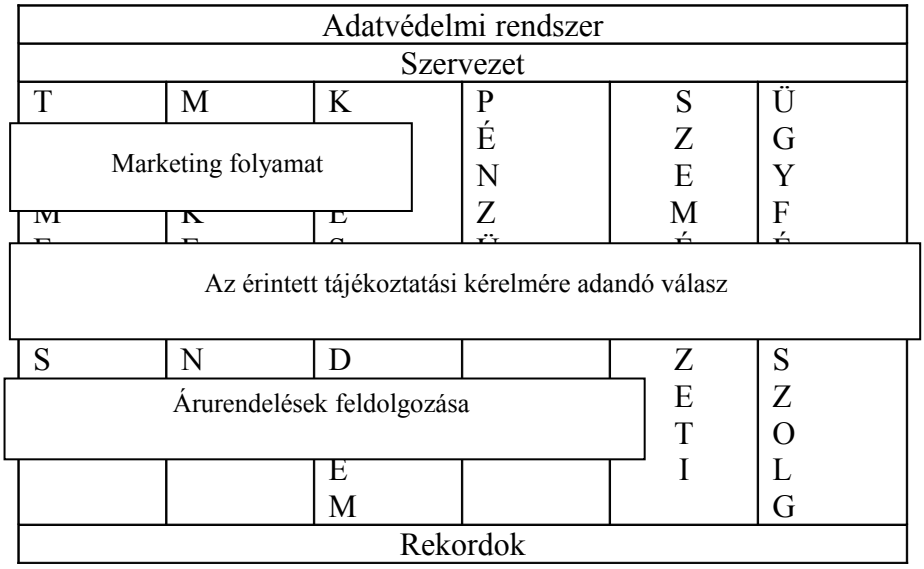
Folyamat- vagy horizontális audit

Ez az audit adott folyamatot vizsgál a kezdetétől a végéig, átlépve területek, funkciók vagy szervezeti egységek határait. Elvégzése során tiszta képet alkothatunk a szervezet működéséről és funkcióiról. Ajánlatos a szervezet tapasztalt, élvonalbeli munkatársaival együttműködve végezni.

A folyamat audit tipikus példája annak az érintett kérelmére induló folyamatnak a vizsgálata, melynek végeredményeképpen az adatkezelő tájékoztatást nyújt az érintett általa kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatairól /Infotv 15. § (1)/. Ebben az esetben e kérelem feldolgozásában minden bizonnyal a szervezett több, különféle egysége is részt vesz. Másik példa, amikor a személyes adatok gyűjtésére használt adatlap tartalmát kívánják módosítani. Ezt általában a marketing részleg kezdeményezi, de rendszerint áthalad

a kereskedelmi, a termelési, a pénzügyi, a jogi és az informatikai részlegeken is, míg végül a belső adatvédelemért felelős munkatárs hagyja jóvá.

Az alábbi ábra az előbbi és más folyamatok auditját szemlélteti. Egyes folyamatokban természetesen más-más szervezeti egységek, s nem feltétlenül valamennyien, érdekeltek.



Együttműködés az alkalmazottakkal
Nem szabad megfeledkeznünk arról, hogy légyen bár a szervezet adatvédelmi rendszere jól megtervezve és dokumentálva, működtetése mégiscsak az alkalmazottakon múlik. Következésképpen az auditor nem végezhet alapos munkát anélkül, hogy párbeszédet folytatna az auditált tevékenységeket végző munkatársakkal, mely párbeszédnek két módja van.

A munkatársakhoz intézett kérdések
Mind a funkcionális, mind a folyamat audit során egy sor kérdést kell intézni a munkatársakhoz. E kérdéseket az K, L, M és N függelék ellenőrzőlistái tartalmazzák. E kérdésekre adott válaszok elegendő bizonysággal szolgálnak arra, hogy az adatfeldolgozó rendszerben ténylegesen az megy végbe, ami a dokumentációjában meg van határozva. Az auditor tulajdonképpen interjúkat készít az alkalmazottakkal, melyekről feljegyzéseket vezet. E feljegyzések elemzése szolgál az audit lényeges megállapításai megfogalmazására. A kérdezés módszerére és az audit egyéb emberi szempontjaira lentebb még kitérünk.

A munkatársak adatvédelmi tudatosságát felmérő interjúk
A munkatársakkal folytatott egyedi interjúk során az auditor speciális információk megszerzésére koncentrál. Emellett azonban szükség van arra is, hogy felmérje az alkalmazottak adatvédelmi tudatosságának általános színvonalát és a személyes adatok védelmét illető elkötelezettségüket. Az auditor e célból

- egyéni, vagy
- csoportos

interjúkat készít a létszámtól és a rendelkezésre álló időtől függően. Lentebb erre vonatkozó útmutatással is szolgálunk, a I függelékben egy sor célszerű kérdést is megfogalmazunk.
Ha személyes – egyéni vagy csoportos – interjúkat az auditor bármilyen okból nem folytathat, még mindig elkészíthet egy kérdőívet a I függelék alapján. Ez azonban csak a végső mentsvár

lehet, mert lényegesen kedvezőtlenebb eredményre vezethet, mint a személyes – szemtől-szembe – kapcsolat.

Az audit folyamata

Az adatvédelmi audit több, különálló tevékenységet vagy fázist felölelő folyamat, amely hosszabb időt vehet igénybe. E folyamat hatékony lebonyolításának előfeltétele a tipikus auditot alkotó öt fázis alapos ismerete:

- az audit tervezése,
- az audit előkészítése,
- a megfelelőségi audit elvégzése,
- jelentés készítése a megfelelőségi auditról,
- utólagos vizsgálatok.

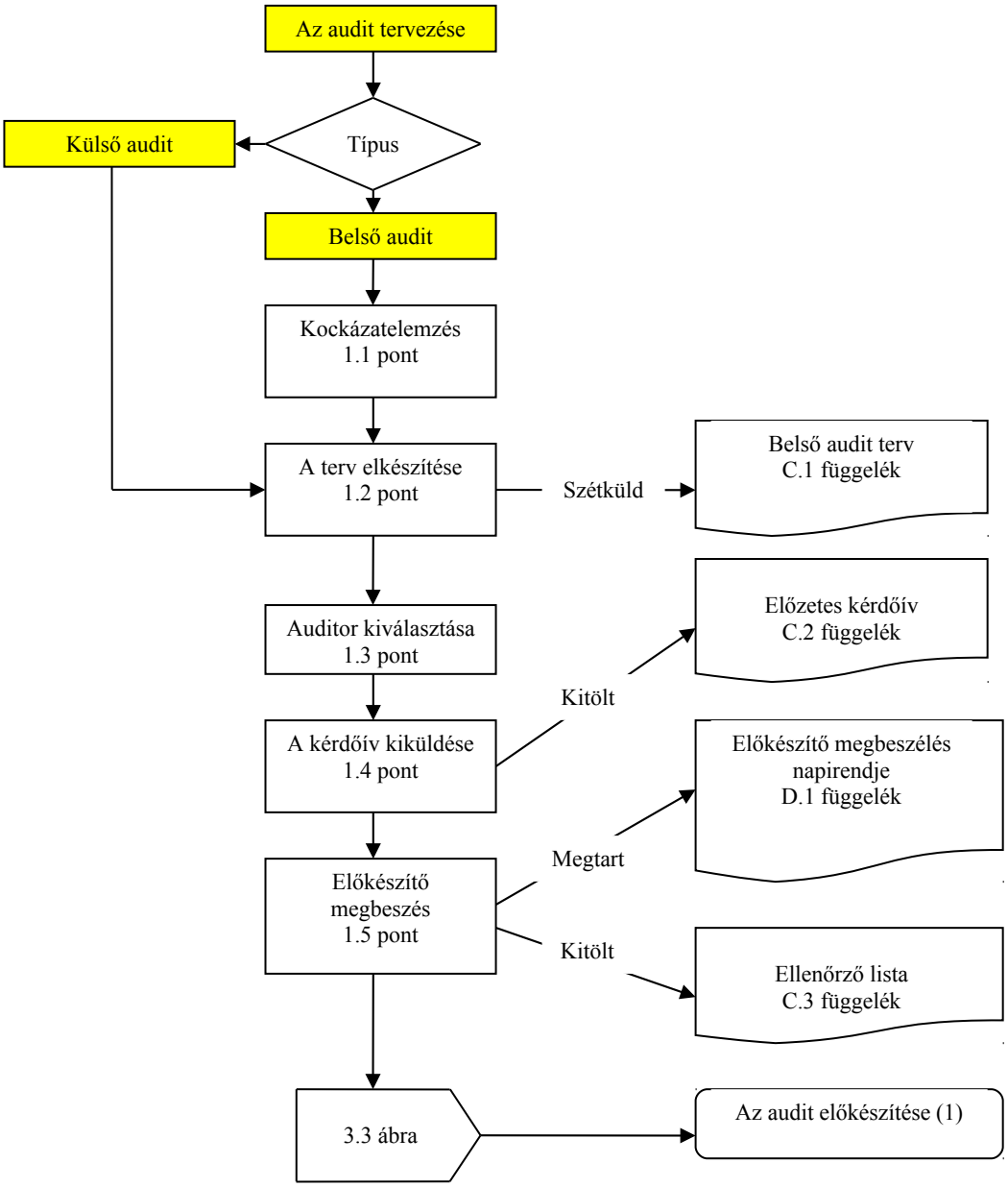
Az alábbiakban ezt az öt fázist időrendi sorrendben részletesen ismertetjük.

az audit tervezése, 3.2 ábra
az audit előkészítése, 3.3 és 3.4 ábra
a megfelelőségi audit elvégzése, 3.5 ábra
jelentés készítése a megfelelőségi auditról, 3.6 ábra
utólagos vizsgálatok. 3.7 ábra

3.1 ábra Az adatvédelmi audit fázisai

1. Az audit tervezése

Minél több munkát fordítunk egy audit tervezésére és előkészítésére, annál zökkenőmentesebben tudjuk majd ténylegesen elvégezni. Az auditra fordított teljes időnek mintegy 25%-át kell ezeknek a kezdeti szakaszoknak szentelnünk, s ha kezdők vagyunk, vagyis először végzünk auditot, akkor még ennél is többet.
A 3.2 ábra a tervezés öt kulcsfontosságú jellemzőjét illusztrálja, melyeket az alábbiakban részletesen ismertetünk. Az 1.1 és az 1.2 pontok csak azokra a szervezetekre vonatkoznak, amelyek az adatvédelmi audit elvégzésére saját belső rendszert kívánnak létrehozni.



3.2 ábra

1.1 Kockázatelemzés

Tapasztalt auditorok – mielőtt az 1.2 pontban részletezett audittervet elkészítik – teljes kockázatelemzést végezhetnek abból a célból, hogy meghatározzák, mely területeket és milyen gyakorisággal kell auditálni. Ennek egyszerű módszerét foglalja össze az A. függelék. Kezdő auditorok és belső adatvédelmi auditot először végző szervezeteknek sokkal egyszerűbb lehet, ha minden egyes funkciót vagy területet ütemterv szerint legalább évente egyszer auditálnak. kézikönyv\A függelék kockázatelemzés.doc bemelve

1.2 Az auditterv

Ha egy szervezet úgy döntött, hogy belső adatvédelmi audit program szerint működik, célszerű éves auditterv készítenie, amely az ellenőrzési mechanizmus lényeges eleme. Az auditterv végrehajtásával gondoskodhatunk arról, hogy a szervezet személyes adatokat kezelő területein tervezett és rendszeres auditot végezzenek. Az auditterv elkészítésének és karbantartásának folyamatát az alábbiakban részletezzük.

1.2.1 Az auditterv elkészítése

Az audittervben rögzítjük, a szervezet mely területeit és mikor auditáljuk. Az első oszlopba az auditálandó területeket, míg az audit gyakoriságát a második oszlopba írhatjuk. A gyakoriságot, ha az nem évente egyszeri, az A. függelékben ismertett módon határozhatjuk meg. A többi oszlop az audit ütemezett időpontját tartalmazza.

Hasznos lehet, ha minden egyes auditnak, időpontja mellett, sorszámot is adunk, így később egyszerűbben hivatkozhatunk rá.

1.2.2 Az auditterv jóváhagyása és ismertetése

Minthogy az auditterv, melyet általában a szervezet adatvédelmi felelőse készít el, a szervezet adatvédelmi megfelelőségi programjának lényeges alkotó eleme, így azt a felsőbb vezetésnek nemcsak ismernie kell, hanem jóvá is kell hagynia. A jóváhagyást követően pedig szét kell küldeni minden szervezeti egység vezetőjének és más érintett személynek.

Egyes, főleg a nagyobb szervezetek esetleg adatvédelmi vagy audit bizottságot is létrehozhatnak, melyek kulcsfontosságú szerepet játszhatnak az auditterv elkészítésében.

1.2.3 Az auditterv karbantartása

Az audittervet évente felül kell vizsgálni, s ha indokolt, módosítani kell. Mindazonáltal előfordulhat, hogy – pl. ha új szervezeti egységet létesítenek vagy az audit gyakoriságát adott területen bármilyen okból módosítani szükséges – az audittervet év közben kell megváltoztatni. Ebben az esetben a módosított tervet is jóvá kell hagynia a felsőbb vezetésnek, s ezt követően meg kell kapnia mindazoknak, akik az előző változatot megküldték. Ha a szervezet minőségbiztosítási rendszert – pl. az ISO 9000 – működtet, az auditterv karbantartását legegyszerűbb a létező ISO 9000 dokumentum ellenőrzővel végeztetni.

1.3 Az auditor kiválasztása

Az adatvédelmi auditokat végző személyek kiválasztásának kulcsfontosságú követelménye, hogy függetlenek legyenek az auditálandó funkciótól. Ez azzal jár, hogy elvileg egy adatvédelemért felelős személy nem auditálhat olyan tevékenységeket, mint az érintett hozzáférésére vonatkozó kérelmek, ha ezeket rendszerint ő maga dolgozza fel. Kisebb szervezetek esetében azonban nehéz vagy lehetetlen a teljes függetlenség, ezért valamiféle kompromisszumos megoldásra kell jutni. Nagyobb szervezetek előnyére szolgálhat, ha a különféle szervezeti egységek munkatársai másik szervezeti egységet auditálnak, ami a legjobb gyakorlat kialakítását segíti elő.

Azoknak az auditoroknak, akik adatvédelmi ellenőrzést végezhetnek, több területen is bizonyos minimális követelményeknek kell megfelelniük. Az ISO 10011-2 szabvány – Minősítési kritériumok minőségügyi rendszerek auditorai számára – nagyon hasznos

kiindulásai pont lehet a szervezetek számára ezeknek a minimális követelményeknek a meghatározásához, amely némi iránymutatást is nyújt mind belső, mind külső auditoroknak.

1.3.1 Az auditorokkal szemben támasztott szakmai követelmények
Az adatvédelmi auditoroknak magas fokú szakértelemmel és az adatvédelem területén szerzett tapasztalatokkal kell rendelkezniük, s képesnek kell lenniük arra, hogy mondanivalójukat, véleményüket, megállapításaikat és javaslataikat mind írásban, mind szóban világosan, közérthetően megfogalmazzák.

1.3.2 Az auditorok képzése
Ideális esetben az auditoroknak megfelelő képzésben kell részesülniük mielőtt bármiféle auditot végeznének.
a) Külső és szolgáltatói auditorok
Egy külső vagy szolgáltatói auditor kiválasztásakor a szervezetnek meg kell győződnie arról, hogy a kiszemelt személyek megfelelő szintű képzésben részesültek, melynek birtokában az auditot meg tudják szervezni és el tudják végezni. A képzés kulcsfontosságú területei:

- az adatvédelmi követelmények alapos ismerete, különös tekintettel az Infotv rendelkezéseire;
- a vizsgálat, a kérdezés, az elemzés, az értékelés és a jelentéskészítés módszereinek mélyreható ismerete;
- az audit lebonyolításához szükséges további gyakorlottság a tervezés, a szervezés, a kommunikáció és az irányítás területén.

b) Belső auditorok
A belső auditorok, mindenekelőtt a kisebb szervezetek esetében, valószínűleg nem részesültek a fentebb körülírt szintű és minőségű képzésben. Ezért a kézikönyv 4. részében a kezdő auditoroknak szolgálunk elegendő iránymutatással ahhoz, hogy további képzés hiányában is alapvető adatvédelmi auditot végezhessenek. A függelék további adatlapjai és ellenőrzőlistái is ezt a célt szolgálják.

1.3.3 Adatvédelmi gyakorlat és tapasztalat
A belső és a külső/szolgáltatói auditorok gyakorlottsága és tapasztalatai az adatvédelem területén széles skálán mozoghat.
a) Ha a szervezet külső vagy szolgáltatói auditort választ, ajánlatos meggyőződnie arról, hogy az auditor tekintélyes tapasztalatokkal rendelkezik az adatvédelem területén.
b) A kisebb szervezeteknek valószínűleg komoly nehézséget jelenthet egy tekintélyes adatvédelmi tapasztalatokkal rendelkező munkatárs alkalmazása, így ismét kompromisszumra van szükség. Nagyobb szervezetek esetében pedig talán csak az adatvédelemért felelős személy rendelkezik megfelelő tapasztalattal, ám ez – az 1.3.1 b) pontban körülírt okból – nem jelentheti egyéb munkatársaknak az auditból való kizárását.

1.3.4 Személyes tulajdonságok
Feladatuk sikeres végrehajtását mind a belső, mind a külső/szolgáltatói adatvédelmi auditorok esetében előmozdítja, ha az alábbi személyes tulajdonságokkal jellemezhetők:

- elfogulatlan és megfontolt,
- gyakorlott elemző, véleménye szabatos és következetes,
- tárgyilagos,
- a különféle helyzeteket reálisan képes értékelni,
- a bonyolult műveleteket széles perspektívába illesztve értelmezi,
- a szervezet egységeinek szerepét egymással összefüggésükben szemléli.

1.4 Az auditot megelőző kérdőíves tájékozódás

Az auditornak – mielőtt az 1.5 pontban ismertetett típusú előzetes megbeszélésre sor kerülne – tanácsos a lehető legtöbb háttér-információt beszereznie. E célból egy kérdőívet kell küldeni a szervezetnek, melyet az a megbeszélést megelőzően kitöltve az auditor rendelkezésére bocsát. A kérdésekre adott válaszokból kitűnik a kezelt adatok és információk neve és jellege, s a szervezetnek módjában áll adatvédelmi tevékenysége bemutatására. A B függelék egy e célra tervezett kérdőívet tartalmaz. kézikönyv Ad 1.4, C.2.doc beemelve
Nagy szervezetek esetében az auditor szükségesnek láthatja, hogy minden egyes szervezeti egység kitöltsön egy kérdőívet. Ennek alapjául szolgálhat a szervezet szervezeti felépítésének ábrája, valamint a szervezeti és működési szabályzata.

1.5 Előkészítő megbeszélés

Az adatvédelmi auditor és a szervezet között az audit megkezdése előtt, végzése során és befejezését követően szoros kapcsolatnak kell lennie. E kapcsolat terjedelme és jellege attól függ, hogy az audit külső, szolgáltatói vagy belső audit.

A belső audit esetében rendszerint csupán arra van szükség, hogy az auditor megvitassa az audit részletkérdéseit (lásd lentebb). A szolgáltatói vagy külső audit esetében egy előkészítő megbeszélést kell tartani a szervezet felelős vezetőivel az audit megkezdését négy-hat héttel megelőzően.

Az előkészítő megbeszélésen az alábbi kérdéseket kell megvitatni:

1.5.1 Adminisztráció

- kapcsolati adatok: a szervezet adatvédelmi munkatársainak megnevezése, akikkel az auditor az auditot megelőzően, az audit végzése során és azt követően kapcsolatot tart;
- az alkalmassági audithoz szükséges dokumentáció kiválasztása és megküldése az auditornak.

1.5.2 Az audit

Az előkészítő megbeszélésen az adatvédelmi audit alábbi szempontjait kell megvitatni és rögzíteni:

- az audit kiterjedése: mely szervezeti egységeket vagy funkciókat érint az audit;
- az audit időtartama: mikor kezdődik és a tervek szerint mikor ér véget;
- az érintett személyek: a szervezet mely munkatársait érinti az audit;
- megbeszélések: hol és mikor lesznek, különösen a nyitó- és a záróértekezlet, és kik vesznek részt rajtuk;
- az audit lebonyolítása: a szervezeti egységek vagy funkciók auditálásának és az audit által érintett munkatársakkal folytatandó megbeszélések időbeli ütemezése;
- jelentés: mikor és milyen – írásos és szóbeli – beszámolót készít vagy tart az auditor a szervezet számára;
- utólagos ellenőrzés: a hiányosságok kiküszöbölésére tett intézkedések megfelelőségének vizsgálatának módja és időpontja.

1.5.3 Praktikus kérdések

Az auditot megelőzően célszerű pontosan meghatározni, hogy az audit végzése során az auditor mely helységekbe léphet be, mely helységet és eszközöket használhatja:

- helyiségek, ahová beléphet;

- helyiség, ahol az audittal kapcsolatos munkát végezheti;
- számítástechnikai eszközök – személyi számítógép, nyomtató, modem stb. – melyeket az auditor használhat;
- telefon, másoló, iratmegsemmisítő stb. használata.

Az előkészítő megbeszélésen megvitatásra javasolt kérdéseket a G függelék tartalmazza. A kezdő auditoroknak további útmutatást nyújt a 4. rész 5. pontja.

1.6 Ellenőrző lista az audit lebonyolításához

Az audit végzése során nagy mennyiségű információt kell áttekintetni és számon tartani. Ezt segítheti egy ellenőrző lista (lásd C.3), melynek egyes rovatai kitöltésével nyomon követhetjük, kivel, mikor, miért tárgyaltunk, milyen dokumentumokból és adatlapokból tájékozódtunk. Ellenőrző lista C.3.doc beemelve mint C függelék

2. Az audit előkészítése

Minél hatékonyabb az előkészítése, annál eredményesebb lesz az audit.

2.1 Az alkalmassági audit

Az audit fentebb már ismertetett módszertana szerint a megfelelőségi auditot megelőzi az alkalmassági audit. Ennek célja kettős:

- értékelni, hogy milyen mértékben felel meg a szervezett adatvédelmi rendszere az Infotv-ben rögzített követelményeknek,
- megbizonyosodni afelől, hogy hozzá lehet látni a megfelelőségi audit elvégzésének, vagy inkább el kell halasztani mindaddig, amíg az alkalmassági audit során megállapított hiányosságokat kijavítják.

2.1.1 Az alkalmassági audit kezdete

Az alkalmassági audit kezdetét az előkészítő megbeszélést követően, a megfelelőségi audit kezdetét két-három héttel megelőző időpontra kell kitűzni.

2.1.2 A dokumentáció áttekintése

A vizsgálat alá tartozó dokumentáció már tárgya volt az előkészítő megbeszélésnek. Tanulmányozása helyileg nem kötődik feltétlenül a szervezethez, kivéve ha csupán a helyszínen hozzáférhető információtechnikai eszközön tárolják. A legfontosabb dokumentációk: szabályzatok, gyakorlati útmutatók, iránymutatások és eljárások. Figyelemmel kell lennünk arra, hogy a szervezet minden, adatvédelemmel kapcsolatos dokumentációját begyűjtsük, függetlenül attól, minek nevezik (pl. banktitok).

2.1.3 Az alkalmassági audit módszere a funkcionális vagy a vertikális audit felettébb egyszerű változata, melynek folyamán

- az auditor gondosan átolvassa a rendelkezésére bocsátott dokumentációt, és
- ellenőrzi, tárgyalja-e mindazon területeket, amelyeket az alkalmassági audit ellenőrző listája (J függelék) tartalmaz. Ez az ellenőrző lista a megfelelőségi audit ellenőrző listáin (K, L és M. függelék) alapul, de azoknak csak a címsorait használja fel, a részletes kérdéseit nem.

2.1.4 Az alkalmassági audit eredménye

A minősítés √, ha a dokumentáció rendben van, ellenkező esetben a minősítés: ∗. Ha a minősítés kérdéses, azt a ? jelzi.
Az audit eredménye „megfelelő”, ha az ellenőrző lista minősítés oszlopában a √ jelek vannak többségben, bár egy-egy ∗ vagy ? is előfordulhat.
Ellenkező esetben az audit eredménye: „nem megfelelő”. Ennek többek között oka lehet:
- hiányoznak vagy nem megfelelőek az Infotv rendelkezéseire való hivatkozások;
- nincsen megfelelően dokumentált adatvédelmi szabályzat;
- hiányzik vagy hiányos azoknak az eljárásoknak a dokumentációja, amelyek különleges adatvédelmi esetekre vonatkoznak.

Mi a teendő? Célszerű az adatkezelőt rábírni, hogy a feltárt hiányosságok kiküszöbölése érdekében intézkedéseket foganatosítson, melyet követően ismételt alkalmassági auditra, s ha az eredményes, a megfelelőségi auditra kerülhet sor. Mindazonáltal az is lehetséges, hogy az adatvédelmi rendszer egyes területeit megfelelőségi auditnak vetjük alá, mielőtt az adatkezelő rendszerét az alkalmassági audit alapján „nem megfelelő”-nek minősítenénk.

2.1.5 Értékelés az alkalmassági audit alapján

A dokumentáció ellenőrzésének eredményét az értékelésben rögzítjük, melyhez a D függelék nyújt segítséget. Az értékelést az ellenőrző listával együtt a szervezet rendelkezésére bocsátjuk, amely egyrészt megjegyzéseket fűzhet az értékeléshez, másrészt intézkedhet a hiányosságok kiküszöböléséről.

2.2 Az auditterv megerősítése

Jól teszi az auditor, ha az audit megkezdése előtt néhány nappal kapcsolatba lép a szervezet által kijelölt adatvédelmi kontaktszeméllyel, s meggyőződik arról, hogy minden, az audit megkezdéséhez szükséges intézkedést megtettek. Ekkor lehet még kisebb változtatásokat is végrehajtani az audit kiterjedését és az auditor rendelkezésére álló belső munkatársakat illetően.

2.3 Az audit ellenőrző listák

Egyéb területek – pl. minőségbiztosítás, pénzügyi rendszerek, IT-biztonság – auditálása során szerzett tapasztalatok azt mutatják, hogy az ellenőrző listák összeállítása és használata a sikeres audit lényeges velejárója. Úgy véljük, ez igaz az adatvédelmi auditra is. Az alábbiakban ezért az adatvédelmi megfelelőségi audit ellenőrző listáival foglalkozunk.

2.3.1 Az audit ellenőrző lista szerepe

Az audit előkészítése és lebonyolítása folyamán, valamint azt követően is jelentős szerephez jutnak az ellenőrző listák:
- segítenek az audit tervezésében és előkészítésében;
- emlékeztetőül szolgálnak az audit lebonyolítása folyamán;
- a lényeges dolgokra összpontosítják figyelmünket;
- segítik az audit irányultságának megőrzését;
- a megjegyzéseinket e listán rögzíthetjük;
- az audit értékelésének alapját képezik.

2.3.2 Az ellenőrző listák hátrányai

Ámbár felettébb hasznosak, ha használatuk megfelelő, helytelen gyakorlat során azonban kellemetlen jelenségek léphetnek fel:
- gátolhatják a rugalmasságot, ha mereven ragaszkodunk előre rögzített tartalmukhoz;

- eltérően szövegezett, de tartalmilag mégis hasonló kérdések már vizsgált ügyek ismételt vizsgálatához vezethetnek;
- ha azokat az auditor csupán mint kérdőíveket használja
    - a szervezet munkatársai hiányolhatják a helyes válaszra irányuló vitát és együttműködést,
    - előbbi következtében fontos területek kimaradhatnak az auditból.

2.3.3 A funkcionális audit ellenőrző listái
Az előbbi hátrányok kiküszöbölésére a funkcionális audit ellenőrző listáit célszerű két féle kérdéskörre alapozni:
- az első kör tartalmazza a visszatérő, minden egyes audit esetében válaszra váró szabványos, előre rögzített kérdéseket;
- a második kör az adott auditra vonatkozó sajátos kérdéseket öleli fel, melyek egy része az auditot megelőzően megfogalmazható, más részük pedig az audit végzése során merülnek fel, s kerülnek az ellenőrző listákra.

Ajánlatos az első kör kérdéseit az audit megkezdése előtt az auditált szervezet munkatársaival előzetesen megvitatni, ami újabb információk megismeréséhez vezethet, s az ezekre vonatkozó kérdésekkel az első kör kiegészíthető.

Az első körbe tartozó kérdések három csoportba oszthatók.
a) A szervezési és vezetési kérdésekkel kapcsolatos három ellenőrző lista (K függelék) tárgya:
- az adatvédelmi rendszer,
- a dokumentáció,
- a fő üzleti folyamatok.

b) A nyolc adatvédelmi elv
A L függelékek nyolc ellenőrző listát tartalmaznak, egyet minden adatvédelmi elvnek.
Általános jellemzőik:
- az egyes elvekkel kapcsolatos fő kérdések újabb kérdéscsoportokat tartalmaznak az adott elv által felölelt adatvédelmi tárgyak szerinti bontásban; e kérdéscsoportok megegyeznek az alkalmassági audit ellenőrző listában már használt kérdéscsoportokkal;
- a kérdéscsoportok általunk megfogalmazott kérdéseit követően az auditor megfogalmazhatja saját, az adott auditra nézve specifikus kérdéseit.

c) Egyéb adatvédelmi kérdések
A M függelék három ellenőrző listája egyéb, általános adatvédelmi szempontokat ölel fel, melyek az auditált szervezet legfelső vezetésére vonatkoznak, s nem az egyes szervezeti egységekre, s az alábbi tárgyakat ölelik fel:
- adatfeldolgozó igénybe vétele,
- bejelentés a nyilvántartásba,
- átmeneti intézkedések.

2.3.4 Folyamat audit ellenőrző lista
Egy adatvédelmi auditnak nem csak a szervezet egyes egységei keretei között működő adatvédelmi rendszereit kell vizsgálnia, hanem ki kell terjednie a szervezeti egységeken túlnyúló kulcsfontosságú működési folyamatokra is. E működési folyamatok többsége minden szervezetre vagy szervezeti egységre nézve egyedi, például azokra a folyamatokra, amely az érintett hozzáférési kérelmét kezelik. A folyamat audit feladata, hogy nyomon kövesse e folyamatok működését, ellenőrizve, hogy az adatvédelmi jogszabályok rendelkezésit azok minden szakaszában betartják.

Bár a 2.3.3 pontban foglaltak alapján úgy tűnik, hogy célszerű jó néhány ellenőrző listát szerkeszteni, ez azonban csak a funkcionális audit megkezdését megelőzően lehetséges, a folyamat audit esetében nem. Az auditornak ezért minden egyes folyamat auditot megelőzően az adott folyamatra vonatkozó ellenőrző listát kell szerkesztenie. Ezt könnyíti meg a N. függelék, amely az előbbi okból üres, kérdéseket nem tartalmaz, hiszen azokat az auditor írja majd bele.

2.3.5 Az ellenőrző lista elkészítése
Az auditornak az ellenőrző lista készítése során az audit alapvető célját kell szem előtt tartania, éspedig:
- objektív bizonyítékot kell szereznie a szervezet vagy a szervezeti egység adatvédelmi rendszere állapotáról, hogy informált ítéletet alkosson annak megfelelőségéről és hatékonyságáról;
- az auditor ezért mintákat vesz a kiválasztott területről, melyek alapján értékeli a rendszer megfelelő és hatékony voltát.
A minták kiválasztásakor az auditor arra törekszik, hogy a minta az audit célját tekintve reprezentatív legyen. Az K, L és M függelék ellenőrző listáinak kiegészítéséhez az auditor segítségére lehetnek az alábbiak:
- ha az adatvédelmi rendszert alaposan dokumentálták, az ellenőrző kérdések egyszerűbbek lehetnek, míg dokumentáció hiányában részletesebbeknek kell lenniük;
- gondoljuk át, mit kell megvizsgálnunk, és mit keresünk;
- a reprezentatív minták kiválasztásakor koncentráljunk a szervezeti egység vagy terület fő funkcióira;
- gondoljunk a priferiális tevékenységekre is, mert ezeket esetleg elhanyagolják, s ezért valószínűbb, hogy az érintettnek sérelmet vagy kárt okoznak;
- helyes megvizsgálni azt is, mi történik, ha
    - sok munkatárs távol van, pl. beteg vagy szabadságát tölti;
    - a munkatársak nagy része lecserélődik;
    - a hónap vége vagy a pénzügyi év vége közeledik;
    - a számítógéprendszer meghibásodik;
    - a munka intenzitása abnormálisan magas, pl. egy biztosítónál, amikor egy nagyobb vihart követően elárasztják a céget a biztosítottak igényei.

2.4 A mintavétel kritériumai

Ha manuális vagy számítógépi fájlokból szükséges rekordokat mintául választani.

2.5 Az audit terv

Az audit előkészítésének ebben a szakaszában az auditor már elkészítheti az audit tervet, amely egyrészt tartalmazza a megfelelőségi audit időbeli ütemezését, másrészt pontosan rögzíti, ki, mit, mikor és hol végezze a tevékenységeket.
Az auditornak viszonylag rövid idő alatt nagy munkát kell elvégeznie, ezért idejét a lehető leghatékonyabban kell beosztania. Az audit tervezésekor ezért célszerű az alábbi helyes gyakorlatot követnie:
- a szervezet adatvédelmi felelősével vagy más vezetőjével tekintsék át a funkcionális audit K, L és M függelékében található ellenőrző listát; ezáltal az auditor megismerkedik a szervezet felépítésével;
- ha ketten auditálnak, a második auditor egyéni és csoportos interjúkat készíthet, mialatt az első a funkcionális auditot végzi;

- az egyéni interjúk alkalmával az auditor kapcsolatba kerül a munkatársakkal és információhoz jut feladataikról, s rögtön ezután – hatékonyan kihasználva ezt a kapcsolatot, és eliminálva az alapvető tájékoztatáshoz szükséges időt – következhet az interjúalany feladatainak folyamat auditja;
- ha csak egy auditor van, úgy a kezdeti funkcionális audit befejezését követően készítheti el az egyéni vagy csoportos intrjúkat, s ezután kezdheti el a folyamat auditot.

3. A megfelelőségi audit folyamata

Az alábbi öt pontban a megfelelőségi audit öt kulcsfontosságú szempontját taglaljuk, melyeket a 3.5 ábrán is szemléltetünk.

3.1 A nyitóértekezlet

A nyitóértekezleten az auditor megbeszéli a szervezet adatvédelemért felelős vezető munkatársaival, mi az audit célja és tárgya az alábbiak szerint:
- az audit hatóköre;
- az audit terv;
- megbeszélések a munkatársakkal, ideértve a záróértekezletet is;
- az audittal érintett adatvédelmi tevékenységet folytató munkatársak kijelölése;
- az audit
- az audit értékelésének elkészítése;
- nyomkövetés;
- gyakorlati kérdések.

3.2 Az auditált környezet

A nyitóértekezletet követően hozzáláthatunk a megfelelőségi audit egyes feladatainak elvégzéséhez. Mindenek előtt győződjünk meg arról, hogy az audit egyes feladatait a legalkalmasabb környezetben a szervezet leghivatottabb munkatársaival végezzük.

3.2.1 Funkcionális vagy vertikális audit

Az audit célja az adatvédelmi rendszer működésének ellenőrzése adott területen, funkción vagy szervezeti egységen belül. A megfelelőségi audit e komponensének alapjául szolgálnak a funkcionális audit ellenőrző listái az K, L és M függelékben. E listák feldolgozását leginkább egy tárgyalóteremben végezhetjük (pl. ott, ahol a nyitóértekezlet volt), vagy az auditszobában.
- Egy tárgyaló ideális hely az adatvédelmi rendszer részletes jellemzőinek feltárására, de arra nem alkalmas, hogy ezek hogyan és milyen hatékonyan valósulnak meg a gyakorlatban. Ezt csupán *in situ* vizsgálhatjuk, kikérdezve a feladatot ténylegesen végző munkatársakat.
- Nagyonis valószínű, hogy a tárgyalóba hozott dokumentációt előzetesen mint a legjobb példát választották ki. Az auditor ezért tekintse meg a teljes dokumentációt, és válassza ki maga, melyeket kíván megvizsgálni.

3.2.2 Folyamat vagy horizontális audit

Az audit során adott folyamat adatvédelmi jellemzőit vizsgáljuk a kezdetétől a végéig. Az auditált folyamat átnyúlik az egyes területeken, funkciókon vagy szervezeti egységeken. Következésképpen az auditor felkeresi mindazokat a helyszíneket, ahol az adott folyamat egy-egy részfeladatát végzik, mely helyszíneket már egyértelműen meghatároztak a nyitó értekezleten. Az auditor a feladatot ténylegesen végző munkatársakat kérdezi ki. El kell kerülni, hogy a szervezeti egység vezetője vagy az adatvédelmi felelős ebbe beavatkozzék és a kérdésekre a munkatárs helyett válaszoljon, kivéve ha erre az auditor kéri.

3.2.3 Interjúk a munkatársak adatvédelmi tudatosságáról
A szervezet adatvédelmi rendszere működésének vizsgálata mellett lényeges meggyőződnünk arról, hogy a személyes adatok rutinszerű kezelését végző munkatársak rendelkeznek-e a feladatuk ellátásához szükséges tudatossággal. Erre leginkább a személyes vagy csoportos interjú a legalkalmasabb. Az interjú során tájékozódhatunk arról is, hogyan oktatták be a munkatársakat.

3.3 Az audit végrehajtása

A megfelelőségi audit módszere változatos attól függően, az audit mely komponensét hajtjuk éppen végre. Az egyes komponensek esetében használható legalkalmasabb módszereket a 3.2 pontban már megismert címszavak szerint tárgyaljuk.

3.3.1 Funkcionális vagy vertikális audit
Az audit egy adott szervezeti egységre korlátozott folyamatokra vagy eljárásokra koncentrál, s nem nyúlik át egyéb szervezeti egységekre. Jó példa erre egy személyzeti osztály valamennyi funkciójának auditja. A 3.2.1 pontban már említett ellenőrző listák – K, L és M függelék – a megfelelőségi audit e komponense esetében is használhatók. Javasoljuk tekintetbe venni az alábbiakat:
a) Kérdezési technikák
Az ellenőrző lista minden egyes kérdése esetében:
- tegyük fel a kérdést, hogy megállapítsuk a tényeket;
- fogalmazzuk meg a választ saját szavainkkal, hogy meggyőződjünk arról, jól értettük-e;
- győződjünk meg arról, hogy a válasz megegyezik azzal, amit az adatvédelmi rendszer ténylegesen tartalmaz;
- rögzítsük írásban megállapításainkat, ahogyan azt a következő pontban javasoljuk.
Készüljünk fel arra, hogy az ellenőrző lista kérdéseinek sorrendjét megváltoztassuk, s esetleg más vagy új kérdéseket is feltegyünk (erre szolgál a listák üresen hagyott helye).
b) Az ellenőrző listák használata
A kitöltött ellenőrző listák rögzítik az audit során feltárt információt, helyes használatát ezért itt is hangsúlyozzuk. Az K – N függelékek ellenőrző listái oszlopai az alábbi, fejlécükben megjelölt információt tartalmazzák
- Dokumentáció: melyet megvizsgáltunk, s mely megállapításainkat igazolja. Ajánlatos rögzíteni a dokumentumot azonosító adatokat (iktatószám, az eljárás, szabályzat pontos megnevezése stb.)
- Ténymegállapítások és megfigyelések: itt rögzítjük, hogyan értékeljük a dokumentációban foglaltakat mint annak igazolását, hogy az adatvédelmi rendszer megfelel az Infotv rendelkezéseinek.
- Minősítés
    - R: megfelelő (rendben),
    - N: súlyosan nemmegfelelő,
    - K: kismértékben nemmegfelelő,
    - M: megfigyelések. Az auditor ugyan nemmegfelelőséget nem állapított meg, de megfigyelt olyan pontenciális problémákat, melyeket kezelni javasol.

3.3.2 Folyamat vagy horizontális audit
Ilyen folyamatra például szolgál az érintett hozzáfésre vonatkozó kérelme, amely több szervezeti egységen is átnyúlik. Ellenőrző listaként a N. függelék használható. A folyamat audit ugyan nagyon hasonlít a funkcionális audithoz, végrehajtásához mégis ajánlatos a kövekezők megfontolása:

a) Kérdezési technikák
Megegyezik a folyamat auditéval /3.3.1 a) pont/. Mindazonáltal fontos megfigyelni, mi történik az egyes kérdések feltevése esetében; így ellenőrízhetjük az megfelel az eljárásnak.
b) A folyamat audit ellenőrző listába – N. függelék – saját kérdéseinket tartalmazza.
Használat a funkcionális audit ellenőrzőlistájával megegyezik az alábbi kiegészítésekkel:
- dokumentumok: a vizsgált dokumentumok azonosító adatain kívül rögzítsük azt is, kit, mit, hol, mikor vizsgáltunk;
- ténymegállapítások és megfigyelések: rögzítsük, mit figyelt meg az auditor, mit mondott az auditált személy, s hogy mindez milyen mértékben felel meg az eljárásoknak.
c) A folyamat audit stratégiája
Az eredményes folyamat audit végrehajtását megkönnyíti egy konzisztens „bejárási" technika. A folyamat ilyetén bejárása során az auditor egy audit nyomvonalat létesít, amely rámutat a folyamattól való eltérésekre. A tevékenység javasolt sorrendje:
- az auditor a folyamatot az egyik végétől a másik járja be, s választása szerint:
    - irány előre: kezdjük a bejárást a folyamat elején, s haladjunk annak befejeztéig, például induljunk az érintett hozzáférési kérelmével, és kövessük a folyamatot, amíg a kért adatokat az érintett rendelkezésére bocsátják;
    - irány visszafelé: kezdjük a bejárást a folyamat végén, s haladjunk visszafelé a kezdetéig, például induljunk az érintett hozzáférési kérelmének teljesítésével, s haladjunk visszafelé a kérelem beérkeztéig.
- ha eltérést találunk, igazolás végett azonnal közöljük az adatvédelmi felelőssel, és folytassuk a bejárást mindaddig, amíg a valószínűsítő okot azonosítjuk. Az audit így hasznosabb a szervezet részére, mintha csak az eltérésről adunk információt, továbbá segíthet a hiba kiküszöbölésében is.
- Az eltérést valószínű okaival együtt rögzítjük a folyamat audit ellenőrző listájában, ahonnan végül átemeljük a 4.2-ben körülírt nem megfelelőségi értékelésbe.

3.3.3 A munkatársak adatvédelmi tudatosságát felmérő interjúk
A megfelelőségi audit során az auditornak fel kell mérnie a szervezeten belül a munkatársak adatvédelmi tudatosságát, és az elkötelezettségüket az adatvédelmi rendszerhez. Erre szolgálnak az egyéni vagy csoportos interjúk.
a) Az interjú alanyainak száma
Egyéni vagy csoportos interjúk esetében meg kell határoznunk, hogy személy legyen az interjúk alanya. Az alábbi táblázat a javasolt minta méretét mutatja:

Az auditált szervezet vagy szervezeti egység munkatársainak száma	Javasolt minta mérete
1-5	100 %
6-15	50 %
16-50	25 %
51-100	15 %
101-500	10 %
501-2500	5 %

A táblázat csupán iránymutatás, a minta méretét az adott szervezet sajátosságaitól függően meg lehet változtatni.
b) Egyéni interjúk
Jellemzői:
- beszélgetés négyszemközt,
- időtartam: 15 – 30 perc,

- strukturált interjú célzatos kérdésekkel,
- a célzatos kérdések lényeges tartalma:
    - szerepek és felelősségek,
    - általános adatvédelmi ismeretek,
    - az interjú alany munkáját érintő adatvédelmi elvek ismerete,
    - a szervezet adatvédelmi rendszerének ismerete,
    - milyen tréningen vett részt,
- az auditor kérdéseinek és az interjú alany válaszainak rögzítésére szolgál a I függelék az egyéni és csoportos interjúk adatlapja.

c) Csoportos interjúk

Jellemzői:

- nagyobb szervezetek vagy szervezeti egységek esetében alkalmazzuk, melyek több munkatársa ugyanazt a feladatot végzi;
- a csoport mérete: a 3.3.3 a) pont táblázata szerint;
- strukturált interjú célzatos kérdésekkel,
- a célzatos kérdések lényeges tartalma:
    - szerepek és felelősségek,
    - általános adatvédelmi ismeretek,
    - az interjú alany munkáját érintő adatvédelmi elvek ismerete,
    - a szervezet adatvédelmi rendszerének ismerete,
    - milyen tréningen vett részt,
- az auditor kérdéseinek és az interjú alany válaszainak rögzítésére szolgál a I függelék az egyéni és csoportos interjúk adatlapja.

c) Csoportos interjúk

Jellemzői:

- nagyobb szervezetek vagy szervezeti egységek esetében alkalmazzuk, melyek több munkatársa ugyanazt a feladatot végzi;
- a csoport mérete: a 3.3.3 a) pont táblázata szerint;
- strukturált interjú célzatos kérdésekkel,
- a célzatos kérdések lényeges tartalma:
    - szerepek és felelősségek,
    - általános adatvédelmi ismeretek,
    - az interjú alany munkáját érintő adatvédelmi elvek ismerete,
    - a szervezet adatvédelmi rendszerének ismerete,
    - milyen tréningen vett részt,
- az auditor kérdéseinek és az interjú alany válaszainak rögzítésére szolgál a I függelék az egyéni és csoportos interjúk adatlapja.

Az egyéni interjúktól eltérően az auditor inkább a mediátor mint a kérdező szerepét tölti be. Így a csoport tagjai beszélgetnek, mely beszélgetést az auditor a kívánt irányba igyekszik terelni. Ugyanakkor vegyük figyelembe, hogy azok, akik úgy vélik, nem tudják a helyes választ, rendszerint hallgatnak, ami amunkatársak ismereteinek általános szintjéről hamis benyomást eredményezhet.

d) Az interjúk lényeges tartalmának rögzítése

Mind az egyéni, mind a csoportos interjúk lényeges tartalmát az egyéni és csoportos interjúk adatlapján – I függelék – rögzítjük. Célszerű elemezni a kitöltött adatlapot, feltárva a hasonló trandeket és attitüdöket. Ha pl. a munkatársak teljes tudatában vannak az adatvédelmi kérdéseknek és a rendszer működésének, úgy munkájukat minden bizonnyal tervszerűen és hatékonyan végzik, és megfelelő tréningben részesültek.

3.3.4 Pozitív auditálás

Megfigyeléseink ellenőrző listán való rögzítése során fontos rögzíteni mindazt, amit megvizsgáltunk, nem csupán a problémákat és a nemmegfelelőségeket. Ezt pozitív auditálásnak nevezzük, hiszen kiegyensúlyozott képet nyújt a teljes auditról, ahelyett hogy csak a hibákra koncentrálnánk. Ha pl. öt dokumentumot vizsgáltunk meg, és egyikükben hibákat fedeztünk fel, rögzítsük a négy hibátlan dokumentum azonosító adatait, valamint a hibásét is. Ezt a gyakorlatot követve egyszerűbb lesz megírni a megfelelőségi audit értékelését, és elkerülhetjük, hogy egy nem tisztességes negatív benyomást okozzunk.

4. A megfelelőségi audit értékelése

Az adatvédelmi audit eredményét formális módon dokumentálni kell és az audit végeztével át kell adni a szervezetnek. Ha az audit értékelését korrekt módon dokumentáljuk, a szervezetet értékes információkhoz jutatjuk adatvédelmi rendszerük státuszáról, melynek főbb tartalma:
- a szervezet auditált területei és az audit időpontja;
- azoknak a területeknek a felsorolása, amelyek megfelelnek az Infotv rendelkezéseinek;
- a törvény rendelkezéseinek nem megfelelő területek, a nem megfelelőség indokolásával, súlyával és kockázataival;
- időben ütemezett programjavaslat a feltárt hibák kijavítására.

A megfelelőségi audit értékelésének öt szempontját az alábbiakban tárgyaljuk, folyamatát a 3.6 ábrán illusztráljuk.
A nem megfelelőség rögzítésére szolgáló adatlapot a E függelék tartalmazza az alábbiak szerint:

4.1 A nem megfelelőség adatlapja

Az audit során feltárt nem megfelelőségeket célszerű a helyszínen azonnal dokumentálni, rögzítve a feltárt hiányosságokat különös tekintettel azok tárgyilagos bizonyságaira. A rögzített információnak választ kell adnia a következő kérdésekre:
- mi (a hiányosság leírása),
- hol (a rendszer mely részében),
- mikor,
- miért,
- ki,
- hogyan.

4.1.1 Fejléc:
- az audit azonosító adatai,
- a nem megfelelőség azonosító adatai,
- a szervezet neve,
- a szervezeti egység, funkció vagy terület megnevezése,
- az audit időpontja.

4.1.2 A nem megfelelőség részletei
Az adatlap e részében egy-egy hiányosság esetében adjunk választ a ki, hol, mikor, miért, kit és hogyan kérdésekre. Itt rögzítjük a hiányosság igazolását megjelölve a hibás rekordokat vagy dokumentumokat, a megfigyelt cselekményeket és a megkérdezett munkatárs nevét. Az adatlap tartalmát a záórértekezleten megvitatjuk és a szervezet vezetőségével jóváhagyatjuk. Fontos tudatában lennünk annak, hogy a megfigyelt hiányosság az eredménye egy folyamatnak és nem az oka. Ezért törekeni kell arra, hogy a igazolása tárgyilagos legyen és egyértelműen a hiányosság okára engedjen következtetni. Jó példa erre, ha az adatgyűjtésre szolgáló adatlap nem nyújt lehetőséget információtartalma nem tisztességes felhasználásának

megakadályozására, mert nem felel meg az első adatvédelmi elvnek. Az auditor ezért vizsgálja meg, a szervezet hogyan ellenőrzi és hagyja jóvá az adatlap tartalmának megfelelőségét. A jóváhagyás legjobb bizonyítéka, ha az adatlapon megjelenik az adatvédelmi vezető aláírása.
Fontos tudatában lennünk annak, hogy a megfigyelt hiányosság az eredménye egy folyamatnak és nem az oka. Ezért törekeni kell arra, hogy a igazolása tárgyilagos legyen és egyértelműen a hiányosság okára engedjen következtetni. Jó példa erre, ha az adatgyűjtésre szolgáló adatlap nem nyújt lehetőséget információtartalma nem tisztességes felhasználásának megakadályozására, mert nem felel meg az első adatvédelmi elvnek. Az auditor ezért vizsgálja meg, a szervezet hogyan ellenőrzi és hagyja jóvá az adatlap tartalmának megfelelőségét. A jóváhagyás legjobb bizonyítéka, ha az adatlapon megjelenik az adatvédelmi vezető aláírása.

4.1.3 A hibajavítási program

Minden egyes nem megfelelőségi adatlap tartalmát meg kell vitatni a záróértekezleten az adatvédelemért felelős vezető munkatársakkal, egyetértésre jutva a hibák kijavításának progamja kérdéseiben (lásd 4.5 pont). Csak ezt követően rögzítjük a programot az adatlapon, az azért felelős munkatársat is megjelölve, az utólagos ellenőrzés (nyomkövetés) dátumával együtt. A kölcsönös egyetértést az auditor és az adatvédelmi vezető aláírásával ismeri el.

4.1.4 A hibák kijavításának utólagos ellenőrzése

Az adatlap alsó részében a hibajavítás utólagos ellenőrzésének részleteit rögzítjük:
- a hibák javítását a megállapodás szerint végrehajtották,
- a nem megfelelőség ismételt előfordulását hatékonyan kiküszöbölték.

Mindezt az auditor és az adatvédelmi vezető aláírása igazolja.

4.2 A nem megfelelőség kategóriái

A nem megfelelőség nem csak azt jelenti, hogy a szervezet adatvédelmi eljárásai nem alkalmasak az adatvédelmi rendelkezések megsértésének megakadályozására, hanem azt is, hogy alkalmasak ugyan, de végrehajtásuk nem korrekt. A C.6 függyelék adatlapja a nem megfelelőség két szintjét különbözteti meg:

4.2.1 Súlyos nem megfelelőség

Az alábbi körülmények esetén:
- az adatvédelmi rendelkezések folyamatos és rendszeres megsértése,
- az érintettre nézve komoly következményekhez vezető hibák (pl. betőhiba a személyes adatokban arra vezethetnek, hogy valakit őrizetbe vesznek);

4.2.2 Kismértékű nem megfelelőség

Az alábbi körülmények esetén:
- az adatvédelmi rendelkezések megsértését időnként emberi hibák okozzák,
- az érintettre nézve csekély következményekhez vezető hibák (pl. bosszantó betőhiba a személyes adatokban).

Megjegyzendő, hogy nagyszámú kismértékű nem megfelelőség ugyanazon a területen rendszerhibához vezethet, így az már súlyos nem megfelelőségnek tekintendő.

4.2.3 Megfigyelések

Az auditált szervezet számára felettébb hasznos, ha az auditor adott folyamat vagy tevékenység megfigyelésének eredményét rögzíti, mert bár tényleges hiányosságot nem tárt fel, javítanivalóra azonban javaslatot tesz. Például: a szervezetnek van ugyan dokumentált eljárása az érintett hozzáférésének kezelésére, de arról nem rendelkezik, hogy ha az illetékes munkatárs szabadságon vagy betegállományban van, ki végezze a feladatot, így azt csak a törvényben rögzített határidőt követően – a munkatárs visszatértével – elégítik ki.
A megfigyeléseket a F függelék adatlapján javasoljuk rögzíteni.

4.3 Megfelelőségi audit értékelés

Függetlenül attól, hogy találtunk-e bármiféle nem megfelelőséget, az értékelést minden megfelelőségi auditot követően el kell készítenünk. E dokumentum célja:
- rögzíti az audit azonosító adatait: dátum, audit hatálya, értékelt területek, az auditban résztvevő munkatársak stb.;
- javaslatot tesz a feltárt hiányosságok kijavítására;
- az utólagos ellenőrzés tárgya és dátuma.

Az értékelés javasolt adatlapját a C.8 függyelék tartalmazza.

4.3.1 Fejléc

A fejléc az audit szokásos adatait tartalmazza:
- az audit azonosító adatai,
- a szervezet neve,
- a szervezeti egység, funkció vagy terület megnevezése,
- dátum.

4.3.2 Az audit értékelésének összefoglalása

Rövid és tényszerű ismertetés az elvégzett auditról, az adatvédelmi rendszer pillanatnyi állapotáról, melynek alapján a szervezet azonnal képet alkothat arról, mi változott az utolsó audit óta (a helyzet javult, romlott, nem változott).

Az összefoglalás legyen a szó szoros értelmében vett értékelés, s nem leírás mindarról – adatvédellmi szabályzatok, eljárások stb – , aminek a szervezet munkatársai tudatában vannak. A hangsúlyt arra kell helyeznünk, hogy milyen jók vagy hatékonyak ezek a dokumentációk, s hogyan érvényesülnek a mindennapi adatkezelési gyakorlatban.

Az egyes értékelések könnyebb összehasonlíthatósága érdekében az alábbi sorrendet javasoljuk követni.

a) Az audit főbb jellemzői:
- hatály: a vizsgált területek, funkciók vagy szervezeti egységek és az auditált folyamatok megnevezése;
- az alkalmassági audit (ha volt ilyen) eredménye;
- a súlyos és kismértékű nem megfelelőségek, valamint a megfigyelések száma.

b) A funkcionális audit értékelése:
- az adatvédelmi rendszer – szervezése, menedzsmentje, dokumentációja – rövid jellemzése és értékelése a szervezet szintjén;
- az adatvédelmi elvek érvényesítése, speciális jellemzők és problémák bemutatása és értékelése.

c) A funkcionális audit specialitásai:
- az adatfeldolgozó minősítése,
- az érintett tájékoztatására szolgáló rendszer minősítése,
- az átmeneti intézkedések minősítése.

d) A folyamat audit értékelése
- minden egyes auditált folyamat rövid bemutatása és minősítése,
- a megvizsgált eljárások, dokumentációk, rekordok stb. felsorolása.

e) Beszámoló az egyéni és csoportos interjúkról
- az egyéni és csoportos interjúk száma,
- a munkatársak elkötelezettsége a magánszféra védelmére és adatvédelmi tudatossága,
- a munkatársaknak tartott adatvédelmi tréningek és hatékonyságuk.

f) A szervezet adatvédelmi rendszere hatékonyságának általános minősítése. Megjegyzések a szervezet általános etikai felfogásáról a személyes információ bizalmas voltát és az adatbiztonságot illetően. Változott-e a helyzet a legutóbbi audit óta?

4.3.3 A hibák kijavítása
- a nem megfelelőség azonosító adatai,

- ki a felelős a hiba kijavításáért,
- a közösen elfogadott hibajavítási program,
- a program befejezésének dátuma.

4.3.4 Utólagos ellenőrzés

A közösen megállapodott utólagos ellenőrzés jellemzői: hatály, időbeli ütemezés stb. (lásd 4.4.4 pont).

4.4 Záróértekezlet

Az auditor
- hangsúlyozza, hogy az audit csupán az adatvédelmi tevékenységekről készített pillanatfelvétel, s a mintavétel is olykor kockázatokat hordoz, mindig fennáll a lehetősége, hogy az audit hatálya alá nem vont területeken vannak nem megfelelőségek.
- összefoglalja az audit értékelését,
- ismerteti megállapításait a szervezet adatvédelmi munkatársaival,
- megállapodik az utólagos ellenőrzés jellemzőiben és időbeli ütemezésében.
- megköszöni a szervezet munkatársainak segítőkész közreműködését.

4.4.1 A nem megfelelőségek megerősítése

Az auditor felolvassa a E függelékben bemutatott adatlapokon rögzített hiányosságokat, melyeket jóváhagyat (esetleges módosítást követően) az adatvédelmi felelőssel.

4.4.2 A hibajavításra tett javaslatok elfogadása

A szervezet felelőssége javaslatot tenni az audit során feltárt nem megfelelőségek kijavítására. Ámbár az auditornak nem feladata tanácsadással vagy útmutatással szolgálni, fontos, hogy a javasolt hibajavítási tervvel egyetértsen.

Végül meg kell határozni a hibajavítás időbeli ütemezését és meg kell állapodni az utólagos ellenőrzés részleteiben is. Az adatlap hiteles voltát az aláírások igazolják.
Ha az audit során nem megfelelőséget nem találtunk, az adatlap üresen marad.

4.5 Utólagos ellenőrzés

Ha az audit során nem megfelelőségeket találtunk, célszerű utólagos ellenőrzést végezni, melynek során meggyőződhetünk arról, hogy a javasolt hibajavítást ténylegesen elvégezték. Az utólagos ellenőrzés folyamatát a 3.7 ábra illusztrálja.

4.5.1 Hatály

Az utólagos ellenőrzés hatályát az feltárt hiányosságok súlya szerint választhatjuk meg:
- kisebb hiányosságok kijavítását telefonon is megerősíthetik,
- a hiányosságok kijavításának dokumentációja megvizsgálása,
- részleges audit lefolytatása azokon a területeken, melyek esetében hiányosságokat találtunk,
- teljes audit azokban a szervezeti egységekben vagy területeken, ahol súlyos hiányosságokat tártunk fel, például a megfelelő belső ellenőrzés hiányát vagy az eljárások rendszeres figyelmen kívül hagyását.

Ezt az információt a megfelelőségi audit értékelés adatlapjának alsó részében rögzítjük a záróértekezleten (lásd 4.4.4 pont).

4.5.2 Időbeli ütemezés

Az utólagos ellenőrzés időbeli ütemezését is a feltárt hiányosságok és a releváns adatvédelmi tevékenységek kockázatának súlya szerint tervezhetjük. A kisebb hiányosságok ellenőrzését elvégezhetjük a következő audit alkalmával is, míg a súlyosak kijavítását minél előbb ellenőrizni kell.

4.5.3 A módszer
Az utólagos ellenőrzés módszerét az 5.1 pontban már ismertett szempontok alapján kell megválasztanunk. Ha csak a dokumentációt kell megvizsgálnunk, elegendő egy alkalmassági audit lefolytatása. Súlyos hiányosság esetében az auditor választhat a fentebb már részletesen tárgyal technikák közül:
- rendszer vagy vertikális audit,
- folyamat vagy horizontális audit,
- interjúk a munkatársakkal.

4.5.4 Az audit lezárása
Miután a szükséges utólagos ellenőrzéseket is lefolytatta, s azokat megfelelőnek találta, az auditot formálisan le kell zárni.
A lezárás formalitásai:
- a nem megfelelőségek adatlapjainak aláírása, ami a hiányosságok kijavítását igazolja,
- a megfelelőségi audit értékelése jóváhagyásának aláírásokkal való igazolása.

5. Audit útmutató

A belső auditorok, különösen a kisebb szervezeteknél feltehetően nem részesültek formális audit tréningben. Mindazonáltal arra biztatjuk e szervezeteket, hogy folyamatosan ellenőrízzék és tökéletesítsék rendszerüket az adatvédelmi rendelkezéseknek való megfelelés érdekében. Ebben a részben gyakorlati tanácsokkal szolgálunk és útmutatót nyújtunk oly módon, hogy még a tréningben nem részesült kezdő auditorok is bátorkodjanak auditot végezni.

5.1 Az auditor szerepe

- a megfelelőség aktuális státuszának ellenőrzése,
- a munkatársak adatvédelmi feladatai ellátásához szükséges tudatosság értékelése,
- a nem megfelelőségek feltárása,
- a kellő korrekciók meghatározása.

Mindezeken túlmenően célszerű figyelembe venni az alábbiakat:
- az auditot végző személy tevékenységét a szervezet felső vezetése teljes mértékben támogatja (ellenkező esetben a munkatársak ellenállását vívhatja ki),
- feladata iránt elkötelezettséget kell mutatnia,
- függetlennek kell lennie az auditált funkciótól, ítéleteiben objektívnek kell lennie.

5.2 Az auditor feladatai

- objektív bizonyítékok tisztességes feltárása és értékelése,
- a megfigyelésekre alapozott általános érvényű következtetések megfogalmazása,
- e következtetések állhatatos védelme azokkal szemben, akik nyomást gyakorolnak rá azzal érvelve, hogy a következtetések nem objektív bizonyítékokon alapulnak,
- az audit folyamatának kitérők nélkül való követése,
- teljes figyelmének koncentrálása az audit folyamatára,

- a megfigyelések és személyes megbeszélések hatékonyságának rendszeres értékelése,
- hatékony reagálás kritikus helyzetekre,
- kollegiális viszony kialakítása az audittal érintett munkatársakkal.

Az első négy pont inkább az audit mechanizmusára, a második négy viszonyt inkább az audit humán szempontjaira vonatkozik. Ez utóbbival a 3. pontban foglalkozunk, az alábbiakban pedig az audit aktuális folyamatára koncentrálunk.

5.2.1 Bizonyítékok gyűjtése

Az auditornak mindig arra kell gondolnia, hogy bármiféle audit alapvető célja objektív bizonyítékok feltárása. Néhány bizonyítékot már a kezdeti alkalmassági audit folyamán is gyűjthetünk a dokumentáció átvizsgálása során. Mindazonáltal arról, hogy a munkatársak a gyakorlatban és ténylegesen hogyan értelmezik és használják az adatvédelmi rendszert, csak úgy győződhetünk meg, ha célzatos kérdéseket intézünk hozzájuk, pl. meginterjuvoljuk őket. Egy csoportos interjú javasolt folyamatát és elemeit a 4.1 ábrán illusztráltuk.

5.2.1.1 Az auditor bemutatkozása

Az auditor néhány szóval bemutatkozik és megköszöni a szervezet munkatársainak, hogy időt szentelnek az auditban való részvételre.

5.2.1.2 Beszélgetés a munkatársakkal

A kezdeti tartózkodás feloldása érdekében az auditor először néhány ártatlan, de releváns kérdést tehet fel, pl. hogy milyen régen dolgoznak a cégnél, mi a személyes feladatuk stb. Jusson eszünkbe, hogy sokaknak stresszel jár, ha auditálják őket, még akkor is, ha az auditor a szervezet munkatársainak egyike.

5.2.1.3 Az audit céljának és lefolytatásának ismertetése

Ennek végeztével ajánlatos és egyúttal tisztességes feltenni a kérdést, mi a véleményük az auditról az munkatársaknak. Ha egy-egy vélemény megalapozott kritikát takar, célszerű az audit tervezett folyamatát módosítani.

5.2.1.4 Információgyűjtés

A beszélgetésre szánt idő túlnyomó részét (legalább 90 %-át) arra kell fordítnunk, hogy minél több információhoz jussunk. Az auditor beszéltesse a munkatársakat, hallgassa meg és jegyezze le a kérdésekre adott válaszokat, tartózkodjék azok minősítésétől.

5.2.1.5 A verbális és a nem verbális információ

Nem árt némi figyelmet fordítani arra, hogyan korrelál a kérdésekre adott verbális és nem verbális válasz, pl.

- az arckifejezés,
- a tekintetek és a szemvillanások kapcsolódása,
- a testmozgás és testhelyzet (pl. bólintás, lehajtott fej),
- viselkedés.

Vegyük észre a nyugtalanságra vagy stresszre utaló jeleket, mert ezek arról tanuskodnak, hogy a munkatársnak nem tetszik, amiről beszélnek, saját válaszai sem őszinték.

5.2.1.6 Összegzés és lezárás

Az auditor

- összegzi a beszélgetés tartalmát, kiemelve a kulcsfontosságú megállapításokat,
- megköszöni a munkatársak aktív részvételét az értékes és érdekes vitában.

5.2.2 A bizonyítékok értékelése
A bizonyítékokat – összegyűjtésüket követően – az auditor tárgyilagosan értékeli, majd döntést hoz arról, megfelelnek-e az Infotv előírásainak vagy nem. Az értékelés során különösen az alábbiakat veszi figyelembe.

5.2.2.1 A források és megbízhatóságuk
A jó döntés feltétele a jó minőségű bizonyíték, melyet a megbízható forrás garantál, amely származhat:
- a dokumentációból,
- személyes vagy
- csoportos interjúkból.
A dokumentáció mint bizonyíték megbízhatóságát több tényező alapján értékelhetjük:
- formális vagy informális dokumentum,
- mikori (ha régi, úgy kevésbé megbízható),
- kitől származik (minél magasabb rangú vezetőtől, annál megbízhatóbb),
- kik kapták meg.
Az interjúk alapján nyert információ megbízhatóságának értékelése során vegyük figyelembe, hogy a válaszadó munkatársak esetleg szeretnek vitatkozni, figyelmezetlenek, tisztességtelenek, elfogultak, türelmetlenek, lusták, közömbösek stb., ugyanakkor lehetnek segítőkészek és együttműködők is, miközben olykor arra törekszenek, hogy azt mondják, amit az auditor hallani szeretne.

5.2.2.2 Az információ megbízhatósága
Fentebb azt fejtegettük, hogyan befolyásolják az audit során gyűjtött információ megbízhatóságát annak forrásai. Nem szabad megfeledkeznünk azonban arról, hogy az információ értékelésére az auditor tárgyilagosságának hiánya is hatással lehet:
- saját szervezetének szemléletmódja,
- korábban végzett auditokból gyűjtött tapasztalatok,
- a legjobb gyakorlatról kialakított saját elképzelések érvényesítése,
- valamiféle, ám elérhetetlen színvonal keresése a törvényes rendelkezéseknek való megfelelés helyett,
- a megfelelési audit során gyűjtött későbbi bizonyítékok gyengítése az alkalmassági audit során nyert kezdeti benyomások által.

5.2.2.3 A bizonyítékok erejének fokozása
Midőn az auditor döntést hoz, minél erősebb bizonyítékokra kell támaszkodnia. A bizonyítékok ereje fokozható:
- ha többször, rendszeresen előfordulnak; az egyszeri előfordulás olykor emberi hiba következménye, míg a többszöri vagy rendszeres előfordulást az adott rendszer vagy folyamat hibás működése is okozhatja.
- háromszögeléssel, vagyis különféle forrásokból gyűjtött bizonyítékok közös részének meghatározásával.

5.2.2.4 Érvényesség, megbízhatóság és ismételhetőség
Egy fontos, nem megfelelőségre utaló bizonyítékot végül célszerű megvizsgálni az alábbi szempontok szerint:
- érvényesség: győződjünk meg arról, hogy a bizonyíték ténylegesen érvényes az értékelt területen, például az Infotv hatálya alá tartozik-e;
- megbízhatóság: győződjünk meg arról, hogy a bizonyíték korrekt és konzisztens, nem mutat a 2.2.1 és 2.2.2 pontban taglalt hiányosságokat;

- ismételhetőség: tegyük fel a kérdést, hogy egy másik auditor ugyanezen bizonyíték alapján ugyanerre a következtetésre jutott volna-e.

5.3. Emberi tényezők
Minthogy a megfelelési audit során gyakorta a szervezet munkatársaival folytatott beszélgetésből gyűjtünk információt, nekik szolgálunk tanáccsal és a helyes gyakorlatra való útmutatással, nem közömbös, milyen magatartási jellemzőkkel rendelkezik az auditor.
Az alábbiakban e jellemzőket foglaljuk össze.

5.3.1 A jó auditor
- tárgyilagos,
- tisztességes,
- alapos,
- jól kommunikál minden szinten,
- barátságos,
- türelmes,
- határozott,
- nyugodt (még ha provokálják is).

5.3.2 A helyes gyakorlat
Néhány tanács:
- kellő körültekintéssel válasszuk ki azt a személyt, aki kérdéseinkre a legjobb választ adhatja. ne vesztegessük időnket azokkal a munkatársakkal, akik nem vesznek részt az adott feladat végrehajtásában vagy nem viselnek felelősséget érte;
- a beszélgetés folyamán nézzünk a megkérdezett személyre, így az könnyebben felfogja a kérdés lényegét, arckifejezése pedig árulkodik arról, érti-e, miről van szó;
- kerüljük a hosszú és bonyolult kérdéseket, fogalmazzunk világosan és egyszerűen;
- fogalmazzunk meg másképpen azt a kérdést, melyet az auditált személy – mint az válaszából is kiderülhet – nem jól értett;
- kerüljük az érzelmi megnyilvánulásokat;
- legyünk pártatlanok, hiszen ítéletünknek objektív bizonyítékokon kell nyugodnia;
- a beszélgetés során alkotott, nem megfelelőségre vonatkozó ítéletünket ne közöljük az auditált személlyel, szorítkozzunk az alapvető tények megismerésére, ellenkező esetben az auditált személy áldozatnak érezheti magát, dühbe jöhet stb.;
- ne legyünk nagyképűek, fennsőbbségesek, ez sértheti a megkérdezett személyt;
- ámbár feladatunk a nem megfelelőség eseteinek felderítése, adjunk hangot elismerésünknek, ha helyes gyakorlatra találunk.

5.3.3 Rossz gyakorlat
- túl sok kérdést teszünk fel egyszerre; csak egy valamit kérdezzünk, s várjuk meg, míg az auditált személy befejezi válaszát, különben összezavarjuk őt;
- ne mondjuk, hogy értjük a választ, ha ez nem igaz; ne féljünk arra kérni az auditált személyt, magyarázza meg bővebben, mit akar mondani;
- saját kérdésünkre ne mi adjunk választ, vagyis ne adjuk a szájába a szavakat;
- kevés időt hagyunk a válaszadásra,
- hangot adunk szubjektív véleményünknek, holott tárgyilagosnak kell lennünk;
- állást foglalunk, holott elfogulatlannak kell lennünk;
- kritizálunk egyes személyeket, esetleg az éppen auditált egyént, holott feladatunk az adatvédelmi rendszer, s nem személyek értékelése (ide értve kritizálását is); ha bizonyítékra találunk az Infotv rendelkezéseinek megsértésére vonatkozóan, először azt vizsgáljuik meg,

nem a rendszernek tulajdonítható-e a sérelem, s ha nem, vagyis emberi mulasztás következménye, vizsgáljuk meg, hogy az auditált személy megfelelő tréningben részeült-e, mert ha nem, úgy ez is rendszerbeli hibának minősül.
Mindezek elkerülhetők, ha mellőzzük a kérdés következő fordulatait:

Fordulat	Valószínű következmény
Az Ön helyében …	szubjektív vélemény
Ha nekem kellene …	előítélet
Ha így jár el ..	tanácsadás
Rendben, de …	vita
Mint mondtam …	kritizálás

5.3.4 Jó kapcsolat kialakítása
Minthogy az audit nagy része az auditált személyhez intézett kérdésekre adott válaszokból gyűjtött információn alapul, nem közömbös, milyen kapcsolatot alakít ki az auditor a megkérdezendő egyénekkel. Néhány jó tanács:
- forduljunk őszinte és barátságos érdeklődéssel az auditált személy felé, hiszen mindenki készségesebben válaszol kérdésekre, ha ezt tapasztalja;
- állítsuk a középpontba az auditált személyt,
- ne adjunk tanácsokat, hiszen nem ez a feladatunk,
- gondoljunk arra, hogy az ember csak azt hallja meg, amit meg akar hallani, s ez ránk is vonatkozik, ezért szó szerint jegyezzük le a kérdéseinkre adott válaszokat;
- értsük meg az auditált személy érzelmeit, attitüdjeit és motivációit;
- ismételjük meg, amit hallottunk, így az auditált személy tanusíthatja annak érvényes voltát;
- vegyük sorra az ellenőrzőlistáinkon előzetesen rögzített kérdéseket.

5.4 Kérdezési technikák
5.4.1 A kérdések alapja
Az audit alkalmával feltett kérdések vagy az auditált szervezet adatvédelmi rendszerének dokumentációján vagy az Infotv követelményein alapulnak. Ezért:
- ne hivatkozzunk helyes gyakorlatokra,
- ne adjunk hangot egyéni preferenciáinknak.
Az audit során ugyanis azt vizsgáljuk, hogy a szervezet különféle területein űzött gyakorlatok és tevékenységek megfelelnek-e az adatvédelmi rendszer dokumentációjában foglaltaknak, s hogy az eleget tesz-e az Infotv követelményeinek.

5.4.2 Jó kérdezési technikák
5.4.2.1 Nyílt kérdések
A nyílt kérdésekre (kiegészítendő kérdés) nem lehet egyszerűen „igen” vagy „nem” választ adni, a válasz ezért informatív lesz.
A nyílt kérdése rendszerint a következő kérdőszavakkal kezdődik: mi, mit, miért, hol, mikor, ki, hogyan stb., és kezdődhet így is:
- megmagyarázná nékem, hogy …;
- mi lenne, ha …. (de a kérdés ne legyen túlságosan hipotetikus).
5.4.2.2 Célzatos kérdések
A beszélgetést az auditor az adott tárgykörre vonatkozó általános kérdéssel indítja, majd fokozatosan szűkíti a következő kérdések sorát.
5.4.2.3 Negatív válaszra indító kérdés
Az auditált személy gyakran kényszert érez arra, hogy a kérdésekre pozitív választ adjon. Ha következő kérdésre pl. mindenki pozitív választ fog adni (bár ezt a „nem” fejezi ki):
- Vétett-e valaha hibát munkája végzése során?

A kérdést átfogalmazva az „igen” válasz elfogadható lesz az auditált személy számára:
- Tévedni emberi dolog. Körül tud-e írni néhány olyan esetet, amikor hibát vétett?

5.4.3 Kerülendő kérdések
5.4.3.1 Zárt kérdések
A zárt kérdésekre (eldöntendő kérdés) adott „igen” vagy „nem” válaszok csekély információt hordoznak az auditor számára, s nem képeznek természetes átmenetet a következő kérdésre.
5.4.3.2 Válaszkorlátozó kérdések
E kérdésekre korlátozott számú – előre tudható – válasz adható. Nem jobb, mint a zárt kérdés.
5.4.3.3 Hipotetikus kérdések
Az efféle kérdésekre adott válasz nem sok információt hordoz az audit számára. Nincs értelme elmélkedésre késztetni az auditált személyt olyan helyzetekről, melyekről nincs tudomása vagy tapasztalata.
5.4.3.4 Rávezető kérdések
E kérdések arra indítják az auditált személyt, hogy válaszuk inkább azt tartalmazza, amit az auditor hallani akar, s nem azt, amit valójában mondani szeretnének.
5.4.3.5 Többszörös kérdések
A kezdő auditorok gyakran több újabb kérdést tesznek fel, mielőtt az auditált személynek ideje lett volna az előzőre válaszolni, így az zavarban van, melyikre is válaszoljon, s nem feltétlenül a legfontosabb kérdésre fog választ adni.

5.4.4 Fekete doboz audit
Előfordulhat, hogy az auditornak egy olyan komplex technikai folyamatot kell auditálnia, melyet kevésbé ismer. Ebben az esetben az auditor a folyamatot fekete doboznak tekintve még mindig ellenőrizheti, hogy a folyamat önmagában megfelel-e az Infotv követelményeinek, vagyis
- a folyamat bemenetét (bemenő információt) megfelelően ellenőrzik-e,
- a folyamat kimenetét (kimenő információt) megfelelően ellenőrzik-e,
- a folyamatot magát megfelelően dokumentálták-e, s az összhangban van-e az érintett személyzet szakmai szintjével;
- megkapta-e a személyzet a folyamat kezeléséhez szükséges tréninget;
- mi történik hiba esetén;
- rögzítik-e a folyamat időbeli lefolyásának főbb adatait, hogy meggyőződhessenek hibamentes voltáról.

5. Az auditor kulcsfontosságú magatartási szabályai
- Az auditor a feladatait tisztességesen és gondosan végzi, ítéleteiben tárgyilagos és elfogulatlan.
- A gyűjtött információ bizalmas voltát megőrzi.
- Tényeket nem titkol el, az audit értékelésében az auditornak ismertetnie kell az audit során feltárt tényeket, különösen azokat, amelyek az adatfeldolgozó rendszer hibáira vagy jogellenes gyakorlatra utalnak.
- Ne vállalkozzon olyan feladatra, amelyhez a szükséges technikai és szakmai ismeretekkel és tapasztalattal nem rendelkezik.

Függelék

A függelék: kockázatelemzés

Ajánlatos a szervezetet olyan, egymástól jól elkülöníthető egységekre bontani, amelyek egymástól függetlenül auditálhatók. Ezt követően mindegyikükre nézve el kell végezni a kockázatelemzést, melynek eredménye alapján meghatározatók a prioritások és az egységek audit alá vonásának gyakoriságai. A nagyobb kockázatot mutató egységeket tanácsos először és gyakrabban auditálni, mint a többit.

A kockázat összetevői
A kockázat nem más, mint az a veszély, amelynek a rendszer ki van téve. Ennek a veszélynek a nagyságát általában bekövetkezése valószínűségével mérik.

A bekövetkezés valószínűsége
Az adatvédelmi rendszer megsértésének valószínűsége: magas (4), közepes (2), alacsony (1).

Következménye
Az adatvédelmi rendszer megsértésének következménye:
- az érintett személyre nézve,
- az adatkezelőre, menedzsereire és alkalmazottaira nézve
rövid és hosszú távon:
súlyos (4), jelentős (2), csekély (1).
A rendszer minősége
A rendszert úgy tervezték, hogy a működése során esetleg fellépő hiba minimális következménnyel járjon a szervezetre nézve:
gyengén tervezett (4), átlagosan tervezett (2), nagyon jól tervezett (1).

A három kockázati összetevőre adott valószínűségi osztályzatok összeszorzásának eredménye – 1 és 64 közé eső szám – felhasználható a relatív prioritás és az audit gyakoriságának meghatározására.

A kockázat egyéb tényezői
Az audit prioritásának és gyakoriságának meghatározását az alábbi tényezők is befolyásolhatják:
- az audit alá vont terület közvetlen kapcsolatban van a szervezet ügyfeleivel, s így jelentős szerepe van kulcsfontosságú tevékenységében;
- az előző audit súlyos gyengeségeket állapított meg a terület adatvédelmi rendszere működésében;
- a terület adatvédelmi rendszerét rövid ideje helyezték üzembe, s még nem volt auditálva;
- a terület adatvédelmi rendszerét nem régen módosították;
- a terület adatvédelmi rendszerének üzemeltetését a közelmúltban új személyzet vette át.

B függelék: előzetes kérdőív

	Kérdőív (kitöltés az auditot megelőzően)	Sorszám:
A szervezet megnevezése		
Szervezeti egység		

Cím		E-mail	
Telefon		Fax	
Kontakt személy neve			
Beosztása, munkaköre			
Tevékenység			
Munkahelyek jellege és száma			
Teljes munkaidőben foglalkoztatottak száma		Részmunkaidőben foglalkoztatottak száma	
Alvállalkozók megnevezése és tevékenysége			
Kérdések			
A személyes adatok feldolgozása természetes személyeket is érint?			
Milyen személyes adatokat gyűjtenek (pl. név, cím, telefonszám)?			
Hogyan tárolják és dolgozzák fel a személyes adatokat: információtechnikai eszközökkel, manuálisan, vagy mindkét módon?			
Mi célt szolgál ezeknek az adatoknak a feldolgozása?			
Nevezze meg és jellemezze a személyes adatokat tartalmazó adatbázisaikat, nyilvántartó rendszereiket!			
Kezelnek-e különleges személyes adatokat (pl. egészségügyi, etnikai), s ha igen, melyeket és milyen célból?			
Hogyan gyűjtik a személyes adatokat?			
Honnan, kitől gyűjtik e személyes adatokat?			
Ki férhet hozzá ezekhez a személyes adatokhoz?			
Továbbítják-e a személyes adatokat más szervezeteknek vagy személyeknek, s ha igen, melyeknek és miért?			
A válaszadó neve és aláírása		Dátum	

C függelék: Ellenőrző lista

	Ellenőrző lista az audit lebonyolításához			
A szervezet neve				
Előkészítő megbeszélés				
A résztvevők neve				
Kérdőív?	Kitöltve? igen nem		A megbeszélés időpontja	

ALKALMASSÁGI AUDIT			
Dokumentáció átvételének dátuma		Az audit befejezé-sének dátuma	
Átvett dokumentumok	Szabályzatok Gyakorlati útmutatók Iránymutatások Eljárások…….Egyéb		
Az audit eredménye	Megfelelő Nem megfelelő		
Megfelelőségi audit	Tervezett időpontja		Nincs tervbe véve
MEGFELELŐSSÉGI AUDIT			
Tényleges kezdete:		Időtartama (napok száma):	
Az audit csoport	vezetője: tagjai		
Az auditot megelőzően gyűjtött vagy készített dokumentáció:			
Kérdőív (1.4 C.2) Rendszeraudit ellenőrző lista Feljegyzések az egyéni és csoportos interjúkról		Auditterv Folyamataudit ellenőrzőlisták Nem megfelelőségi adatok Megfelelőségi audit értékelések	
Az előkészítő értekezlet résztvevői			
Súlyosan nem megfelelt esetek száma:		Csekéllyé nem megfelelt esetek száma:	
Kritikai megállapítások száma:		Egyéni interjúk száma:	
Csoportos interjúk száma:		Megfelelőségi audit értékelés átadva:	
A záró értekezlet résztvevői:			
UTÓLAGOS ELLENŐRZÉS			
Tervezett időpontja:		Tényleges kezdete:	
Az audit csoport	vezetője: tagjai		
Minden súlyos nem megfelelőség javítva:		Minden csekély nem megfelelőség javítva:	
Az audit befejeződött:		Az auditot nem fejeződött be, mert	
Feljegyzések:			

D függelék: Értékelés az alkalmassági audit alapján

Értékelés az alkalmassági audit alapján		
Szervezet:	Szervezeti egység:	Dátum:
A dokumentáció vizsgálatának összefoglaló értékelése		

Nemmegfelelő dokumentumok és tisztázandó kérdések			
Dokumentum	Tisztázandók		
Az audit minősítése			
Megfelelő: az audit a megfelelőségi audittal folytatható			
Nemmegfelelő: a megfelelőségi audit csak azt követően kezdhető meg, ha a szervezet a kisebb súlyú tisztázandó kérdésekkel összhangban a kellő intézkedéseket foganatosította.			
Nemmegfelelő: a tisztázandó kérdések súlyos problémákra mutatnak, az adatvédelmi rendszer jelen állapotában megfelelőségi auditra nem ajánlott.			
Javaslat a megfelelőségi auditra			
Becsült időigénye: (nap)		Az auditcsoport javasolt létszáma: (fő)	
Kezdetének javasolt időpontja:			
Az auditor neve és aláírása:		Dátum:	

E függelék: nem megfelelőség adatlapja

Nem megfelelőség adatlapja			
Szervezet		Audit azonosító	
Szervezeti egység		Nem megfelelőség azonosító	
		Dátum	
A nem megfelelőség részletezése			
A nem megfelelőség kategóriája	Csekély	Nagyfokú	
Az auditor neve	Aláírása	Dátum	

Hibajavítási program		
	Aláírás	Dátum
Auditor		
AV felelős		
Utólagos ellenőrzés		
A hibajavítás utólagos ellenőrzése		
	Aláírás	Dátum
Auditor		
AV felelős		

F függelék: megfigyelések adatlapja

Megfigyelés			
Szervezet		Audit azonosító	
Szervezeti egység		Megfigyelés azonosító	
		Dátum	
Részletezése			

Az auditor neve	Aláírása	Dátum
Utólagos ellenőrzés (ha szükséges)		

	Aláírás	Dátum
Auditor		
AV felelős		
Utólagos ellenőrzés		

G függelék: előkészítő megbeszélés napirendje

1. Kezdetek
- Személyes ismerkedés a felsővezetéssel és az adatvédelmi munkát végző munkatársakkal.
- Jegyezzük fel, ki a kontaktszemély az auditot megelőzően, annak folyamán és befejezését követően.
2. Adatkezelési tevékenységek
- Különítsük el a szervezetnek azokat a tevékenységeit, amelyekre az Infotv rendelkezései vonatkoznak az alábbi kérdésekre adott válaszok alapján:
- Ki irányítja a szervezet adatkezelési tevékenységét?
- Mely szervezeti egységek végzik a tényleges adatfeldolgozásokat?
- A feldolgozott adatok fajtái, különös tekintettel a különleges adatokra.
- A feldolgozás módja: kézi, gépi.
- Az adatok felhasználása speciális célokra (pl. hirdetés, közvetlen üzletszerzés).
3. Alkalmassági audit
- Beszéljük meg, milyen dokumentációt és mikor bocsát a szervezet az auditor rendelkezésére az alkalmassági auditot megelőzően?
- Ismertessük azokat a lehetőségeket, amelyeket egy nemmegfelelő minősítésű audit esetén a szervezet választhat.
4. A megfelelőségi audit érintettjei
- Vitassuk meg és rögzítsük, mely szervezeti egységeket vagy funkciókat érint az audit.
- Határozzuk kezdő és tervezett befejezésének időpontját.
- Állapodjunk meg abban, kikre vagy mely csoportokra vonatkozzék az audit.
5. A megfelelőségi audit menete
- Határozzuk meg a nyitó és a záró értekezlet időpontját, helyszínét és résztvevőit.

- Tűzzük ki azokat az időpontokat, amikor az aditor felkeresi az érintett szervezeti egységeket vagy funkciókat, s nevesítsük azokat a munkatársakat, akik az auditor rendelkezésére állnak.
- Ismertessük, az audit befejeztével milyen írásos vagy szóbeli tájékoztatást bocsát az auditor a szervezet részére.
- Beszéljük meg az audit lezárását követő utólagos audit vagy felülvizsgálat lehetőségét, célját (pl. a feltárt hiányosságok kiküszöbölése vizsgálata), időpontját.

6. Gyakorlati kérdések tisztázása
- Mely helyiségekbe léphet be az auditor?
- Biztosítanak-e részére dolgozószobát?
- Mely IT- és egyéb eszközökhöz férhet hozzá vagy használhat (számítógép, nyomtató, telefon, másoló, fax stb.)?

7. Az audit által érintett terület bejárása

Felettébb ajánlatos ezzel zárni az előkészítő megbeszélést, melynek folyamán az auditor
- megismerkedik az épület szerkezetével, a szervezet tevékenységével;
- megtekinti az adatvédelmi rendszer működtetetésének helyiségeit és eszközeit;
- mindezek alapján könnyebb lesz elkészítenie az audit terv első változatát, megbecsülni az audithoz szükséges létszámot, szakértelmet, időtartamot.

H függelék: a nyitóértekezlet napirendje

A nyitóértekezleten az auditor megbeszéli a szervezet adatvédelemért felelős vezető munkatársaival, mi az audit célja és tárgya, továbbá megerősíti a megfelelőségi audit részleteit, melyet kezdetben már megvitattak az előkészítő megbeszélésen. A javasolt napirend:

1. Bevezetés

2. Az audit hatóköre
- határozzuk meg az audit által érintett szervezeti egységeket és funkciókat;
- jelöljük ki a szervezet azon munkatársait, akik az audit során rendelkezésünkre állnak, továbbá az adatvédelmi tudatosságról készülő egyéni és csoportos interjúk alanyait.

3. Az audit lebonyolítása
- erősítsük meg a szervezeti egységek és funkciók felkeresésének időbeli ütemezését, és jelöljük ki, mely munkatársak állnak rendelkezésre az egyes szakaszokban, majd adjuk át az audit tervet az érintetteknek;
- erősítsük meg a záró értekezlet időpontját és helyét, valamint határozzuk meg a résztvevőket;
- állapodjunk meg abban, milyen írott vagy szóbeli formában számolunk be az elvégzett auditról, vagyis a megfelelőségi audit értékeléséről és az ehhez csatolt nemmegfelelőségi értékelésről;
- vitassuk meg az esetleges utólagos ellenőrzés (nyomkövetés) lehetőségét, melynek során meggyőződhetünk arról, hogy végrehajtották a szükséges korrekciókat.

4. Gyakorlati kérdések
- keressük fel az auditor számára kijelölt helyiséget;
- vegyük számba az e helységben rendelkezésünkre álló információtechnikai és egyéb eszközöket.

I függelék: egyéni és csoportos interjúk adatlapja

Egyéni és csoportos interjúk adatlapja		
Szervezet:	Szervezeti egység:	
Auditor:	Audit azonosító:	Dátum:
Résztvevők		
Név	Pozíció	Munkaviszonyának kezdete
Az interjú kérdései és a kérdésekre adott válaszok		
1. Mit tud mondani nékem az Infotv-ről?		
Válasz:		
2. Mit jelent Önnek az adatvédelem kifejezés?		
Válasz:		
3. Az Ön által használt adatok közül melyeket tekint „személyes adat”-nak?		
Válasz:		
4. Az Ön által használt adatok közül melyeket tekint „különleges személyes adat”-nak?		
Válasz:		
5. Ismertesse szervezete vagy szervezeti egysége milyen szabályzatok vagy eljárások alapján kezeli vagy használja az efféle adatokat?		
Válasz:		
6. Hogyan befolyásolják e szabályzatok vagy eljárások az Ön egyéni munkáját?		
Válasz:		
7. Milyen tréningen vett részt és milyen útmutatást kapott munkája végzéséhez? (Tekintsük ennek dokumentációját, pl. kézikönyvet, szabályzatot stb.)		
Válasz:		
8. Hogyan gyűjti Ön vagy szervezeti egysége a személyes adatokat és a különleges személyes adatokat?		
Válasz:		
9. Hol tartják vagy tárolják ezeket az adatokat (pl. irattartó szekrényben, adatbázisokban,		

stb.)
Válasz:
10. Mi a forrása ezeknek az adatoknak (pl. állami nyilvántartások, szolgáltatási szerződések, marketing listák, más szervezeti egységek stb.).
Válasz:
11. Van-e jogosultsága arra, hogy ezeket az adatokat továbbítsa vagy közölje szervezetén belül vagy azon kívülre? Ha igen, ismertesse ennek eljárását!
Válasz:
12. ismertesse szervezeti egysége biztonsági eljárásait, pl. a) milyen gyakran változtatja meg jelszavát, b) hogyan gondoskodnak az adatok biztonságos kezeléséről, c) hogyan törlik vagy semmisítik meg a személyes és különleges adatokat?
Válasz:

J függelék: alkalmassági audit ellenőrző lista

Alkalmassági audit ellenőrző lista			
Szervezet:	Szervezeti egység:		Dátum:
Tárgy: **szervezés és vezetés**		Auditor:	
Az adatvédelmi rendszer			
Tárgykör	Dokumentáció	Ténymegállapítások és megjegyzések	Minősítés*
Adatvédelmi szabályzat			
Szervezeti felosztás			
Tudatosság és oktatás			
Tervezés és megvalósítás			
Rendszer audit			
Dokumentáció			
Adatvédelmi eljárások			
Munkakori leírások			
Adatgyűjtés			
Kulcsfontosságú folyamatok			
Kulcsfontosságú folyamatok			
Szervezet:	Szervezeti egység:		Dátum:
Tárgy: **a nyolc adatvédelmi elv**		Auditor:	
Az első elv			
A személyes adatok fajtái			
Feldolgozásuk törvényes alapja			
Különleges adatok feldolgozásának törvényes alapja			
Személyes adatok gyűjtése			

* A minősítés √, ha a dokumentáció rendben van, ellenkező esetben a minősítés: ∗. Ha a minősítés kérdéses, azt a ? jelzi.

Törvényes feldolgozás			
Tisztességes feldolgozás			
Kivételek az első elv alól			
A második elv			
Személyes adatok felhasználása a szervezeten belül			
Meglévő adatok felhasználása egyéb és új célokra			
Az adatok kiadása (továbbítása, közlése)			
A harmadik elv			
Az adat a célhoz szükséges, elérésére alkalmas			
A negyedik elv			
Az adatok pontosak, teljesek			
Az adatok naprakészek			
Az ötödik elv			
Az adatmegőrzés szabályai			
Az adatok megőrzésének felülvizsgálata és törlése			
A hatodik elv			
Az érintett tájékoztatása az adatkezelés megkezdése előtt			
Tájékoztatás az érintett kérelmére			
Helyesbítés			
Törlés, zárolás			
Adattovábbítás			
Nem teljesített kérelmek			
Az érintett tiltakozása			
Automatizált döntés			
A személyzet adatvédelmi tudatossága			
A hetedik elv			
Biztonsági szabályzat			
Jogosulatlan hozzáférés			
A személyzet megbízhatósága			
Véletlen adatvesztés, -sérülés			
Szervezési intézkedések			
Technikai intézkedések			
A nyolcadik elv			
Adattovábbítás külföldi címzettjei			
Továbbítás az érintett hozzájárulása alapján			
Tárgy: **adatfeldolgozó megbízása**		Auditor:	
Az adatfeldolgozó kiválasztása			
Az eredeti szerződés			
A módosítások indoka			
A hatályos szerződés			
Tárgy: **bejelentés a nyilvántartásba**		Auditor:	
Az eredeti bejelentés			
Változások bejelentése			
Tárgy: **az adatkezelési rendszer fejlesztése**		Auditor:	
Jogszabályi változás miatt			
A rendszer tökéletesítése céljából			

K függelék: Megfelelőségi audit ellenőrző lista: szervezési és vezetési kérdések

Megfelelőségi audit ellenőrző lista: szervezési és vezetési kérdések			
Szervezet:	Szervezeti egység:	Dátum:	
Tárgy: **szervezés és vezetés**	Auditor:		
1. Az adatvédelmi rendszer			
Tárgykör	Dokumentáció	Ténymegállapítások és megjegyzések	Minősítés*
1.1 Adatvédelmi szabályzat (helyes gyakorlat, csak megjegyzések)			
a) Van-e a szervezetnek jól dokumentált adatvédelmi szabályzata?			
b) Világosan rögzíti-e a szabályzat a szervezet fő adatvédelmi céljait és azok követelményeit?			
c) Kötelezi-e a szabályzat a szervezetet, hogy a cél eléréséhez szükséges forrásokról gondoskodjék?			
d) A szabályzatot a felső vezetés - támogatja, - minden munkatárs megkapja. A felülvizsgálat gyakorisága és oka?			
e) Rögzíti-e a szabályzat, - miért van szükség e dokumentumra; és - mi azzal a felső vezetés szándéka?			
f) Rögzíti-e a szabályzat az adatvédelmi munkatársak - alá-fölé rendeltségét, - egyéb szabályzatokhoz és folyamatokhoz (pl. oktatás, adatbiztonság, minőségbiz-tosítás) fűződő kapcsolatait?			
g) Definiál-e a szabályzat fegyelmi vétséget, ha a munkatárs nem tartja be az előírásait?			
1.2 Alá-fölé rendeltségi viszonyok			
a) Van-e a szervezetnek az adatvédelmi szabályzat hatékony érvényesítését szolgáló, az alá-fölé rendeltségi viszonyokat rögzítő szerkezeti rendje?			
b) Hogyan határozza meg ez a szerkezeti rend a személyes adatokhoz hozzáférő munkatársak feladatait és felelősségét?			
c) Hogyan biztosítja ez a szerkezeti rend az adatvédelmet illetően a hatékony, a szervezet egészére kiterjedő kommunikációt?			

* R: megfelelő (rendben), N: súlyosan nemmegfelelő, K: kismértékben nemmegfelelő, M: megjegyzés.

d) Megbízta-e a szervezet egyik munkatársát, hogy általános felelősségi körében – mint belső adatvédelmi felelős vagy adatvédelmi felsővezető – az adatvédelmi előírások betartását ellenőrizze és segítse?			
e) Munkaköri leírása részletesen és teljes körűen tartalmazza-e mindezt?			
1.3 A munkatársak adatvédelmi tudatossága és oktatása			
a) Hogyan gondoskodik a szervezet arról, hogy minden, személyes adatokat kezelő munkatárs rendelkezzék a szükséges adatvédelmi tudatossággal és az ehhez elengedhetetlen oktatásban részesüljön?			
b) Mely menedzserek és munkatársak részesülnek oktatásban?			
c) Mi az oktatás tárgya és módszere?			
1.4 Tervezés és megvalósítás (Helyes gyakorlat – csak megjegyzések)			
a) Hogyan biztosítja a szervezet, hogy adatvédelmi szabályzatát tervezett és rendszeres módon megvalósítsák?			
b) Van-e a szervezetnek valamiféle adatvédelmi bizottsága vagy fóruma az adatvédelmi kérdések kezelésére?			
c) Ha van adatvédelmi bizottság - mi az elnevezése, - vannak-e tagjai a felső vezetés köréből, - tagjai-e a szervezet üzletágai személyes adatokat felhasználó munkatársai?			
d) Ha van adatvédelmi bizottság, van-e egy adatvédelmi képviselője, pl. az adatvédelmi felsővezető vagy belső adatvédelmi felelős?			
e) Ha van adatvédelmi bizottság, vannak-e egyéb funkciót ellátó tagjai, pl. auditorok, jogtanácsosok, információtechnikai munkatársak?			
f) Ha van adatvédelmi bizottság - mi a rendeltetése, - mely kérdésekkel foglalkozott a közelmúltban?			
g) Ha van adatvédelmi bizottság			

- mely útmutatókat és folyamatokat vizsgált a közelmúltban, - kivizsgálta-e az adatvédelmi eljárások megsértésének eseteit (említsünk példákat)?			
h) Ha van adatvédelmi bizottság - tesz-e javaslatot a hiányosságok kijavítására, megállapítja-e prioritásukat és időbeli ütemezésüket (említsünk példákat), - készít-e emlékeztetőt tevékenységéről?			
1.5 Rendszer audit és felülvizsgálat (Helyes gyakorlat – csak megjegyzések)			
a) Aláveti-e a szervezet adatvédelmi rendszerét rendszeres auditnak és felülvizsgálatnak, s ha igen, milyen gyakorisággal?			
b) Van-e a szervezetnek dokumentált eljárása a belső adatvédelmi audit lebonyolítására?			
c) Van-e a szervezetnek auditora, aki megfelelő képzettséggel rendelkezik a belső adatvédelmi audit elvégzésre?			
d) Ha a szervezetnek van képzett auditora, független-e az auditált funkciótól?			
e) Dokumentálják-e a belső adatvédelmi audit megállapításait?			
f) Közlik-e a belső adatvédelmi audit megállapításait a hibák és hiányosságok kijavításáért felelős munkatársakkal?			
g) Áttekinti-e a felső vezetés a belső adatvédelmi audit megállapításait?			
h) Javult-e a rendszer a belső adatvédelmi audit megállapításaira épülő fejlesztések eredményeképpen?			
2 A dokumentáció			
2.1 Adatvédelmi eljárások (helyes gyakorlat, csak megjegyzések)			
a) Meghatározta és elkészítette-e a formális dokumentációját azoknak az intézkedéseknek és folyamatoknak, amelyek az adatvédelmi szabályzat megvalósítását szolgálják?			
b) Ha a szervezet elkészítette a folyamatoknak ezt a formális dokumentációját, megkapták-e mindazon munkatársak, akiknek tartalmát ismerniük kell? c) Rendszeresen			

felülvizsgálja-e a szervezet, pl. belső adatvédelmi audit révén, ezt a dokumentációt?			
d) Ellenőrzi-e a szervezet ezt a dokumentációt egy dokumentum ellenőrző rendszerrel, pl. az ISO 9000-rel?			
2.2 Munkaköri leírások és munkavállalói szerződések (helyes gyakorlat, csak megjegyzések)			
a) Világosan meg vannak-e határozva a személyes adatok kezelését végző munkatársaknak az Infotv-ben rögzített felelőssége és kötelezettségei munkaköri leírásukban vagy munkavállalói szerződéseikben?			
b) Az adatok megfelelő védelméhez szükséges folyamatok és eljárások világosan körül vannak-e írva az adatkezelést végző munkatársak munkaköri leírásában?			
2.3 Adatgyűjtés			
a) Ha megváltoztatják az adatgyűjtési adatlapokat vagy a szoftvert, hogyan és milyen módon ellenőrzik használatba vételüket megelőzően az Infotv-nek való megfelelőségüket?			
b) Ha új adatlapot terveznek adatgyűjtési célra, hogyan ellenőrzik adatvédelmi megfelelőségüket?			
c) Ha új szoftvert szándékoznak alkalmazni adatgyűjtési célra, hogyan ellenőrzik adatvédelmi megfelelőségüket?			
3 Fő üzleti folyamatok			
a) Hogyan és mikor veszik figyelembe az Infotv rendelkezéseit új üzleti folyamatok tervezésekor?			
b) Hogyan és mikor veszik figyelembe az Infotv rendelkezéseit új üzleti folyamatokat támogató új hardver eszköz specifikációja, beszerzése és tesztelése során?			
c) Hogyan és mikor veszik figyelembe az Infotv rendelkezéseit új üzleti folyamatokat támogató új szoftver specifikációja, beszerzése és tesztelése során?			
d) Hogyan integrálja az adatvédelmi rendszer a kulcsfontosságú nemzetközi szabványokat, köztük - az ISO 27001			

adatbiztonsági szabványt, - az ISO 1400 környezetvédelmi szabványt, - az ISO 9000 vállalati minőségbiztosítási szabványt, - az ISO 9001:2000 egészségügyi szabványt.			
e) Integrál-e az adatvédelmi rendszer egyéb, adatkezelési ipari szabványokat, s ha igen, melyeket és hogyan?			
f) Integrál-e az adatvédelmi rendszer egyéb magatartási kódexeket vagy szabványokat, s ha igen, melyeket és hogyan?			

L függelék: megfelelőségi audit ellenőrző lista: a nyolc adatvédelmi elv

Megfelelőségi audit ellenőrző lista: a nyolc adatvédelmi alapelv			
Szervezet:	Szervezeti egység:		Dátum:
Tárgy: **1: az első elv**		Auditor:	
Kérdés	Vizsgált dokumentumok	Tények és megállapítások	Eredmény
1.1 A személyes adatok fajtái			
a) A feldolgozott személyes adatok fajtái? Nevezze meg a feldolgozott különleges adatokat is!			
b) Megkülönböztetik-e a különleges személyes adatokat egyéb személyes adatoktól? ba) Ha igen, hogyan? bb) Ha nem, miért nem?			
c) A különleges adatok feldolgozását a szervezeten belül egyéb személyes adatoktól eltérően végzik-e, s ha igen, hogyan?			
1.2 A személyes adatok feldolgozásának jogalapja			
a) Meghatározták-e a személyes adatok feldolgozásának jogalapját, s ha igen, hogyan? Sorolja fel e jogalapok mindegyikét!			
b) Meghatározták-e a személyes adatok feldolgozásának célját, s ha igen, hogyan? Sorolja fel e célok mindegyikét!			
c) A személyes adatok feldolgozásának jogi alapjait megkülönböztetik-e azok fajtái szerint, s ha igen, hogyan?			
1.4 Hozzájárulás az adatkezeléshez			
a) Ha a személyes adatok feldolgozásának jogalapja az			

érintett hozzájárulása, mikor és hogyan szerzik meg ezt a hozzájárulást?			
b) Ha a személyes adatok feldolgozásának jogalapja az érintett határozott hozzájárulása, mikor és hogyan szerzik meg ezt a hozzájárulást?			
1.5 A feldolgozás törvényes feltételei			
A közigazgatási szférához tartozó szervezetek: a) A személyes adatok feldolgozását törvény vagy önkormányzati rendelet alapján végzik-e? Ha igen, nevezzék meg, melyek azok! b) Figyelembe veszik-e a feldolgozás során az emberi jogokat, különös tekintettel a természetes személy magánszférájának tiszteletben tartására?			
Valamennyi szervezet: c) A személyes adatok feldolgozása során a szervezeten belül eleget tesznek-e a bizalmasság követelményének?			
d) Hogyan értelmezik ezt a bizalmasságot?			
e) Mik e bizalmas kezelés garanciái (pl. a közlésre vagy megsemmisítésre vonatkozó szabályok)?			
f) Adatkezelésükre vonatkoznak-e egyéb törvények vagy rendeletek?			
g) Ha igen, melyek és miért?			
h) Hogyan érvényesíti e törvények és rendeletek előírásait?			
1.6 Tisztességes feldolgozás követelményei			
a) Hogyan tájékoztatják az érintetteket arról, hogy adataik kezelője szervezetük?			
b) Mikor tájékoztatják erről az érintetteket?			
c) Hogyan tájékoztatják az érintetteket személyes adataik felhasználásának céljáról?			
d) Mikor tájékoztatják erről az érintetteket?			
e) Felajánlják-e az érintetteknek azt a lehetőséget, hogy megtiltsák adataik felhasználását egyéb célokra?			
f) Mikor ajánlják fel ezt a lehetőséget?			
g) Nyújtanak-e egyéb információt az érintetteknek adatkezelésükről? Ha igen, mit tartalmaz ez az információ?			
h) Hogyan és mikor nyújtják			

ezt az információt?			
i) Fogadnak-e az érintettre vonatkozó információt harmadik felektől? Ha igen, melyeket? Ha nem, ugorjunk a G.1.7 pontra!			
j) Ha fogadnak az érintettre vonatkozó információt harmadik felektől, hogyan és mikor tájékoztatják őt erről?			
1.7 Kivételek az első adatvédelmi elv alól			
Az Infotv szerint az adatkezelő kötelessége az érintettet tájékoztatni az alábbiakról: 1. az adatkezelőt azonosító adatokról (hiszen az érintett csak ennek tudatában érvényesítheti vele szemben jogait); 2. a belső adatvédelmi felelős azonosító adatairól, ha ilyet az adatkezelő kinevezett (hiszen az érintett csak így tud panaszával hozzá fordulni); 3. az adatok feldolgozásának céljáról; 4. minden egyéb információról, ami az adatok feldolgozásának sajátos körülményeire vonatkozik (pl. adattovábbítás).			
a) Megkapják-e az érintettek mindezeket az információkat? Ha mindig megkapják, ugorjunk a G.2.1 pontra. Ha nem, milyen kivételek képezik ennek jogi alapját?			
b) Hogyan határozták meg ezeket a kivételeket?			
c) Hogyan értékeli e kivételek megvalósítását?			
2 A második elv			
2.1 Személyes adatok felhasználása a szervezeten belül			
a) Milyen eljárásokkal vezetik a személyes adatok felhasználásának mindenre kiterjedő és naprakész nyilvántartását?			
b) Milyen gyakorisággal ellenőrzik ezt a nyilvántartást?			
c) Kiterjed-e ez a nyilvántartás minden olyan eszközre, amely személyes adatok feldolgozását végzi, és azokra a feldolgozással érintett fájlrendszerekre, amelyek ezeket az adatokat tartalmazzák?			
d) Kiterjed-e a nyilvántartás a szervezet által megbízott adatfeldolgozóra?			
2.2 Az érintett tájékoztatása Notifying the Data Subject			
a) Milyen eljárást követve tájékoztatják az érintettet arról (ha ez szükséges), hogy személyes adatai feldolgozását milyen célból fogják végezni? Infotv 20.§			
2.3 A NAIH tájékoztatása			
2.4 A meglévő személyes adatok felhasználása új célokra			
a) Hogyan tájékoztatják a meglévő személyes adatok felhasználásának újabb céljairól - a szervezet tájékoztatásért			

felelős munkatársát, - az érintettet, - a NAIH-t:			
b) Ellenőrzik-e és hogyan, az újabb cél összeegyeztethető-e az eredeti céllal?			
2.5 A tájékoztatás karbantartása			
2.6 Az adatok közlése, továbbítása			
a) Van-e szabályzatuk az adatok közlésére szervezeten belül és továbbítására harmadik felek részére?			
b) Dokumentálták-e ezt a szabályzatot?			
c) Hogyan tudatosítják ezt a szabályzatot a munkatársakban, beoktatják-e őket a közlés és a továbbítás feltételeiről?			
d) Hogyan tudatják az érintettel/adatalannyal, hogy személyes adataik közlésre vagy továbbításra kerülnek?			
e) Mérlegeli-e, hogy a továbbított személyes adatokat a harmadik fél a jogszabályi előírások betartásával kezeli? Ha nem, ugorjunk a g.3.1 pontra!			
f) Ha igen, hogyan végzik el ezt a mérlegelést?			
3 A harmadik elv			
3.1 A személyes adatok elengedhetetlen és megfelelő volta			
a) Miért, mi célból kezelnek személyes adatokat?			
b) Hogyan döntik el, hogy a személyes adatok minden egyes célból elengedhetetlenül szükségesek?			
c) Hogyan döntik el, hogy a meghatározott célból gyűjtött személyes adatok megfelelnek-e ennek a célnak, a cél elérésére alkalmasak, azt nem haladják meg?			
d) Milyen eljárások szolgálnak annak periodikus ellenőrzésére, hogy az adatgyűjtési eljárások során csak a célhoz elengedhetetlen, megfelelő és a cél elérését meg nem haladó adatokat gyűjtsék? Milyen gyakran vizsgálják felül ezeket az eljárásokat?			
e) Vannek-e eljárásaik annak értékelésére, hogy a gyűjtött adatok mennyisége és fajtái az adott céllal összhangban vannak? Ha igen, melyek ezek?			
f) Vannak-e állományaikban olyan személyes adatok, amelyek csak egyes tételek esetében megfelelőek?			

g) Ha a munkatársak megjegyzést fűzhetnek egyes tételekhez, milyen eligazítást kapnak ahhoz, hogy e megjegyzések megfelelőek legyenek?			
4 A negyedik elv			
4.1 A személyes adatok pontossága és teljessége (4.§/4)			
a) Értékelik-e a személyes adatokat abból a szempontból, hogy mekkora kárt okozhat az érintettnek és az adatkezelőnek pontatlan vagy nem teljes voltuk?			
b) Hogyan és milyen gyakran ellenőrzik a személyes adatok pontosságát és teljességét? Említsenek példákat!			
c) Milyen esetekben fordulnak az érintetthez személyes adataik pontosságának és teljességének ellenőrzése céljából? Említsenek példákat!			
d) Ellenőrzik-e a személyes adatok pontosságát és teljességét, amikor azokat nem az érintettől, hanem egyéb forrásból gyűjtik? Ha igen, hogyan?			
e) Megnevezik-e a személyes adatok forrását (érintett, felhasználó vagy harmadik fél) az adatállományban? Ha igen, hogyan? Említsenek példákat!			
f) Rögzítek-e, ha az érintett kifogásolja adatai pontosságát vagy teljességét?			
4.2 A személyes adatok naprakészsége			
a) Értékelik-e a személyes adatokat abból a szempontból, hogy mekkora kárt okozhat az érintettnek és az adatkezelőnek nem naprakész voltuk?			
b) Van-e eljárásuk annak meghatározására, mikor és milyen gyakran szükséges a személyes adatok naprakészségéről gondoskodni?			
c) Van-e nyomkövető eljárásuk az érintettre vonatkozó megjegyzések vagy egyéb észrevételek relevanciája, ténybeli pontossága és időszerűsége ellenőrzésére?			
d) Duplikálnak-e és kezelnek-e adatokat különálló szervezeti egységek különböző helyeken? Ha igen, hogyan közlik az ilyen duplikátumokat kezelő felekkel a frissítéseket és módosításokat?			
e) Hogyan informálják a			

személyes adatok módosításáról azokat a harmadik feleket, melyeknek az adatokat továbbították?			
f) Hogyan kezelik az adatok naprakészségére vonatkozó panaszokat?			
Az adatok pontosak, teljesek			
Az adatok naprakészek			
5 Az ötödik elv			
5.1 Az adatmegőrzés szabályai			
a) Milyen kritériumok szerint határozzák meg a személyes adatok megőrzésének időtartamát és milyen gyakran vizsgálják felül ezeket a kritériumokat?			
b) Érvényesítik-e ezeket a kritériumokat a gyakorlatban?			
c) Rögzítik-e a személyes adatok létrehozásának vagy felvételének időpontját?			
d) Rendszereik beépített módon gondoskodnak-e a megőrzés időtartamának kezeléséről? Ha igen, élnek-e ezzel a lehetőséggel?			
e) Van-e jogszabályi kötelezettségük a megőrzésé időtartamára vonatkozóan? Ha igen, nevezze meg őket!			
f) Vannak-e ágazatspecifikus szabályok a megőrzésre vonatkozóan? Ha igen, nevezzék meg őket!			
5.2 A személyes adatok felülvizsgálata és törlése			
a) Van-e szabályzatuk a felülvizsgálatra vonatkozóan? Ha van, dokumentálták is?			
b) Ha már nem szükséges egy adott célból gyűjtött adatok megőrzése - hogyan vizsgálják felül az adatokat annak meghatározására, hogy melyeket kell törölni? - milyen gyakran végzik el az adatok felülvizsgálását? - a szervezet mely munkatársa felelős e felülvizsgálatért? - ha a személyes adatokat számítógépen tárolják, az alkalmazási program megjelöli-e azokat az adatrekordokat, melyeket felül kel vizsgálni vagy törölni kell?			
c) Felülvizsgálják-e időnként a személyes adatokat annak meghatározására, hogy - szükség van-e archiválásukra? - megőrizhetők-e anonimizált formában (pl. történeti vagy			

statisztikai célra?			
d) Adódnak-e olyan kivételes körülmények, amikor egyes adatokat a szokásos időtartamon túl is megőriznek? Melyek ezek a kivételek? Ki határozza meg e kivételeket (név, beosztás)?			
5.3 A személyes adatok törlése			
a) Milyen eljárást követnek a személyes adatok törlése során, ha az adatkezelés célja megszűnik?			
b) Mi a gyakorlatuk személyes adatok törlése, megsemmisítése során (pl. selejtezés)? Más-e ez a gyakorlat különleges személyes adatok esetében?			
6 A hatodik elv			
6.1 Az érintett hozzáférése			
a) Hogyan azonosítják az érintett személyes adatai kezelését illető tájékoztatásra vonatkozó kérelmét?			
b) Hogyan azonosítják a kérelmezőt?			
c) Igényelnek-e információt az érintettől, hogy meghatározzák a kért információ lelőhelyét? Ha igen, milyen információt kérnek?			
d) Hogyan határozza meg a lelőhelyét a kérelemben megjelölt személyes adatokhoz (ide értve valamennyi hozzáférhető rekordot)?			
e) A kérelem beérkezését követően folytatják-e a kérelemben megjelölt személyes adatok rutinszerű feldolgozását?			
f) Ha ez a feldolgozás a kérelemben megjelölt információ módosítására vagy törlésére irányul, hogyan kezelik ezt az érintett vonatkozásában?			
g) Mit tartalmaz a kérelemre adott válasz?			
h) Hogyan közlik az érintettel az információt?			
i) Hogyan adnak az érintettnek megfelelő információt arról, miként végzik a feldolgozást?			
j) Adnak-e az érintettnek másolatot a szervezetük által tárolt információról?			
k) Ha az érintett megelégszik azzal, hogy csupán megtekintse ezt az információt, hogyan mutatják ezt be?			
m) Ha a válasz egyes részei nem közérthetők, szolgálnak-e			

magyarázattal egyes kódokat vagy más, az érintett számára nem érthető információkat illetően? Ha igen, hogyan?			
n) Tartalmaz-e a kérelem alapján gyűjtött információ harmadik félre vonatkozó vagy harmadik felet azonosító adatokat?			
o) Kiadják-e a kérelmezőnek harmadik félre vonatkozó információt?			
p) Ha nem adnak ki a kérelmezőnek harmadik félre vonatkozó információt, mi annak indoka?			
q) Hogyan gondoskodnak arról, hogy a kérelmezőnek a törvényes határidőn belül válaszoljanak?			
6.2 Az érintett kérelmének elutasítása			
a) Mely esetekben tagadják meg az érintett kérelmében foglalt személyes adatokhoz való hozzáférésre vonatkozó tájékoztatást? Hogyan indokolják?			
b) A megtagadás az érintett hozzáférését korlátozó kivételeken alapul? Ha nem, ugorjunk a 6.3 pontra: Ha igen, hogyan határozzák meg ezeket a kivételeket?			
c) Értékelik-e a kivételek relevanciáját? Ha igen, hogyan és a szervezet mely munkatársai?			
d) Ha az érintett hozzáférését személyes adataihoz megtagadják, az Infotv mely rendelkezéseire hivatkoznak?			
6.3 Jogsérelmet vagy kárt okozó feldolgozások			
a) Van-e eljárásuk a személyes adatok feldolgozásának ellenőrzésére, mielőtt a feldolgozást ténylegesen megkezdik?			
b) Az eljárás tartalmazza-e a feldolgozás ellenőrzését az érintettnek okozott jogsérelem kiküszöbölése érdekében?			
c) Figyelembe veszik-e, hogy az érintettnek okozott jogsérelem vagy kár esetében az érintett kártérítést követelhet és jogorvoslatért az adatkezelő ellen bírósághoz fordulhat?			
d) Felhívják-e a munkatársak figyelmét ezekre a lehetőségekre? Ha igen, hogyan?			
e) Van-e tudomásuk arról, hogy egyes működő feldolgozásuk jogsérelmet vagy kárt okozhat az érintettnek?			

Ha igen, milyet?			
f) Milyen eljárást követnek, ha az érintett kártérítést követel vagy bírósághoz fordul?			
g) Eljárásuk rögzíti-e az érintett tiltakozására adandó válasz tizenöt napos határidejét?			
6.4 A tiltakozás joga			
a) Milyen eljárást követnek, ha az érintett tiltakozik adatai feldolgozása ellen, pl. közvetlen üzletszerzési célra vagy egyéb okból?			
b) A közvetlen üzletszerzést célzó adatállományok tartalmazzák-e az érintett preferenciáit (levélposta, fax, telefon, SMS)?			
6.5 Automatizált adatfeldolgozással hozott döntés (11.§)			
a) Rendszerük hoz-e az érintettre vonatkozó döntést, amely kizárólag automatizuált feldolgozáson alapul? Ha igen, mely törvény mely rendelkezése alapján?			
b) Ha igen, milyen eljárást követve tájékoztatják az érintettet erről?			
c) Milyen eljárást követve és mennyi időn belül adnak tájékoztatást az érintett kérelmére, az alkalmazott módszerről és annak lényegéről?			
d) Milyen lehetőséget biztosítanak az érintettnek álláspontja kifejtésére?			
6.6 Helyesbítés, törlés, zárolás, megsemmisítés (21.§, 22.§/5, 61.§/1)			
a) Milyen eljárást követve végzik a személyes adatok - helyesbítését, - zárolását, - törlését vagy - megsemmisítését, ha az érintett erre vonatkozó kérelmének helyt adnak, vagy azt a NAIH vagy a bíróság elrendeli?			
b) Milyen eljárást követve értesítik azokat a harmadik feleket, melyeknek személyes adatot továbbítottak, e személyes adatok helyesbítéséről, zárolásáról törléséről vagy megsemmisítéséről?			
6.7 A munkatársak adatvédelmi tudatossága és oktatása			
a) Hogyan készítik fel a munkatársakat arra, hogy felfigyeljenek az érintett hozzáférés kérelmére?			
b) Hogyan készítik fel a munkatársakat arra, hogy válaszoljanak az érintett hozzáférés kérelmére?			

Lásd még: F.1.3 függelék: A munkatársak adatvédelmi tudatossága és oktatása			
7 A hetedik elv			
7.1 Biztonsági szabályzat			
a) Van-e adatbiztonsági szabályzatuk? Ha igen, mutassák be!			
b) Mely szervezeti egységük és munkatársuk felelős az adatbiztonsági szabályzat összeállításáért és érvényesítéséért?			
c) Megakadályozza-e a szabályzat gyakorlati alkalmazása az érintettnek esetlegesen okozott jogsérelem és adataihoz való illetéktelen hozzáférés lehetőségét?			
d) Figyelembe veszik-e a biztonsági megoldások a technikai fejlődés legújabb termékeit és ezek alkalmazásának költségeit?			
e) Milyen gyakorisággal és eljárással vizsgálják felül a biztonsági szabályzatot?			
f) Szabályzatuk mely specifikus adatvédelmi rendelkezésekre épül?			
g) Alkalmazzák-e az ISO 27001 adatbiztonsági szabványt vagy más biztonsági szabványt vagy helyes gyakorlatot? Ha igen, melyeket?			
h) Hogyan felügyelik, hogy a szervezeten belül megfelelően alkalmazzák az adatbiztonsági szabályzatot?			
i) Milyen gyakran és mely szervezeti egységük vagy munkatársuk ellenőrzi az adatbiztonsági szabályzat betartását?			
j) Van-e eljárásuk a szabályzat be nem tartásának kezelésére? Ha igen, milyen?			
k) Az adatbiztonsági szabályzat a teljes szervezetre vonatkozik? Ha nem, mely szervezeti egységre nem és miért?			
l) Van-e egyéb biztonsági szabályzatuk vagy eljárásuk, amely azokra a munkatársakra vagy szervezeti egységekre vonatkozik, amelyek az általános biztonsági szabályzatot nem alkalmazzák? Ha igen, mely szervezeti egységek vagy munkatársak ezek?			
7.2 Adatok illetéktelen vagy jogellenes feldolgozása			
a) Meghatározza-e biztonsági szabályzatuk, mi minősül illetéktelen vagy jogellenes			

feldolgozásnak? Ha igen, hogyan? Ha nem miért nem?			
b) Milyen biztonsági intézkedésekkel előzik meg az adatokhoz való illetéktelen vagy jogosulatlan hozzáférést a szervezeten belül (pl. jelszavas hozzáférés)?			
c) Vannak-e fokozott biztonsági intézkedéseik a különleges adatokhoz való illetéktelen vagy jogosulatlan hozzáférés megakadályozására? Ha igen, melyek ezek?			
d) Milyen eljárással észlelik a biztonsági intézkedések megsértését?			
7.3 A munkatársak megbízhatósága			
a) Ismertetik-e a személyes adatok feldolgozását végző munkatársakkal a biztonsági szabályzatot?			
b) Beoktatják-e a munkatársakat a biztonság- és kockázatkezelés gyakorlatáról? Ha igen, mit tartalmaz ez az oktatás?			
c) Mely szervezeti egységek munkatársai és milyen gyakran részesülnek ebben az oktatásban?			
d) Dokumentálják-e az oktatás anyagát útmutatóban vagy kézikönyvben, hogy arra a jövőben hivatkozhassanak? Ha igen, mutassák be őket!			
e) Milyen intézkedésekkel korlátozzák, hogy a személyes adatokhoz csak a feljogosított munkatársak férhessenek hozzá? Úgy pl., hogy megállapítják feladatuk ellátásához való szükségességét?			
f) Az egyes szervezeti egységek maguk ellenőrzik a személyes adatokhoz való hozzáférési jogosultságot, vagy ezt központosítják?			
g) Hogyan korlátozzák, hogy csak a feljogosított munkatársak férjenek hozzá a rendszerekhez vagy léphessenek be helyiségekbe?			
h) Feljogosítják-e a munkatársakat, hogy eszközt (pl. laptopot) vagy szoftvert a szervezeten kívül eső helyen használjanak vagy munkájukat otthon végezzék? Ha igen, milyen különleges utasítások szerint kell gondoskodniuk az adatok biztonságáról?			

Mutassanak be példákat!			
7.4 Személyes adatok megsemmisítése			
a) A már nem szükséges személyes adatok megsemmisítése során hogyan akadályozzák meg az azokhoz való illetéktelen hozzáférést?			
b) Van-e az előbbitől különböző eljárásuk a különleges adatok megsemmisítésére?			
Lásd még: 5.3 A személyes adatok törlése			
7.5 Kontingencia-tervezés – véletlen adatvesztés, megsemmisülés, sérülés			
a) Van-e kontingencia-tervük előre nem látható események kezelésére?			
b) Ha igen, tesztelték-e ezt a tervet? Milyen gyakran? A tesztelés eredménye alapján módosították-e a tervet, s ha igen, hogyan?			
c) Tájékoztatják-e és milyen gyakran a munkatársakat a kontingencia eljárásáról?			
d) Mentik-e háttértárra a személyes adatokat (back-up)? Ha igen, on vagy off site? Hol van ez a háttértár?			
e) A tesztelést az aktuális adatokon végzik-e? Ha igen, milyen eljárással védik a személyes adatokat a tesztelés folyamán?			
f) Milyen kockázatkezelési eljárásuk van azoknak az adatoknak a visszaállítására, amelyek sérültek vagy elvesztek az alábbi okokból: - emberi hiba, - számítógépvírus, - hálózati hiba, - lopás, - tűz, - árvíz, - egyéb katasztrófa?			
8 A nyolcadik elv			
8.1 Megfelelő szintű védelem			
a) Hogyan értelmezik a védelem szintjének megfelelőségét?			
b) Továbbítanak-e személyes adatokat az EGT-n kívül eső országba vagy térségbe? Ha igen, hová? Ha nem, úgy nincs több kérdésünk a 8.1 ponttal kapcsolatban.			
c) Mi a célja a külföldre irányuló adattovábbításnak?			
d) Milyen típusú adatokat			

továbbítanak (pl. kapcsolati adatok, alkalmazottak adatai)?			
e) Továbbítanak-e külföldre különleges személyes adatokat? Ha igen, melyeket?			
f) Milyen kockázatokkal jár a személyes adatok továbbítása az EGT-n kívüli országokba?			
g) Milyen intézkedésekkel gondoskodnak a megfelelő biztonságról, amikor az adatokat másik országba vagy térségbe továbbítják?			
h) Ellenőrizték-e, s ha igen, hogyan, hogy a nem EGT-állam megfelelő szintű védelmet nyújt?			
8.2 Kivételes adattovábbítás			
a) Továbbítanak-e személyes adatokat abban az esetben, ha úgy döntenek, hogy a továbbítás kivételt képez a nyolcadik elv alól?			
b) Ha igen, milyen adatokat továbbítanak?			
c) Mely országba vagy térségbe irányul ez az adattovábbítás?			
d) Milyen kritériumok alapján döntenek arról, hogy a továbbítás kivételt képez a nyolcadik elv alól (pl. az érintett hozzájárulása)?			

M. függelék: megfelelőségi audit ellenőrző lista: egyéb adatvédelmi kérdések

Megfelelőségi audit ellenőrző lista: egyéb adatvédelmi kérdések			
Szervezet:	Szervezeti egység:		Dátum:
Tárgy: **1: adatfeldolgozó igénybe vétele**		Auditor:	
Kérdés	Vizsgált dokumentumok	Tények és megállapítások	Eredmény
1.1 Az adatfeldolgozó megválasztása			
a) Hogyan választják ki az adatfeldolgozójukat? A kiválasztás feltétele-e, hogy az adatfeldolgozó megfelelő biztonsági garanciákat nyújtson?			
b) Milyen ésszerű intézkedésekkel biztosítják, hogy az adatfeldolgozó teljesítse az adatvédelmi követelményeket?			
c) Hogyan értékelték ezeknek az adatbiztonsági követelményeknek a teljesülését (pl. kockázatelemzési eljárásokkal).			
d) Hogyan gondoskodnak arról, hogy az adatfeldolgozó ténylegesen teljesítse ezeket a követelményeket?			
e) Van-e eljárásuk eme adatbiztonsági követelmények folyamatos nyomonkövetésére?			
f) Hogyan működik ez az eljárás?			
1.2 Az adatfeldolgozóval kötött szerződés			
a) Tartalmaz-e sajátos adatvédelmi vagy biztonsági előírásokat, pl. az alábbiakra vonatkozóan: - tájékoztatás (pl. az adatok felhasználójáról); - korlátozások (pl. az adatok megismerhetősége és felhasználása); - kötelezettség a megállapított korlátozások betartására; - a vonatkozó adatbiztonsági és adatvédelmi sztenderdek alkalmazása.			
b) A szerződést írásba foglalták-e?			
c) A szerződés tartalmaz-e kikötést, mely szerint a feldolgozó csak a szervezet utasításait hajthatja végre és meg kell felelnie a szervezet által előírt biztonsági kötelezettségeknek?			
1.3 A szerződés felülvizsgálása			
a) Hogyan vizsgálják felül, hogy a szerződés minden szükséges követelményt tartalmaz-e?			

b) Hogyan dokumentálják a szerződés felülvizsgálatát?			
c) Ha audit-követelményeket is megállapítanak, hogyan végzik és értékelik az auditot?			
1.4 A szerződés módosítása			
a) Hogyan és mely esetben kezdeményezik a szerződés módosítását, ki van erre felhatalmazva, és hogyan hajtják végre?			
b) Ki a felelős azoknak az eljárásoknak vagy sztenderdeknek a módosításáért, amelyeket nem megfelelőnek találnak?			
c) A szerződés lejárta vagy felbontása esetén milyen eljárással kezelik a tárolt személyes adatokat (pl. ki tartja meg azokat és mi lesz a sorsuk)?			
1.5 A szerződés megszegése			
a) Mi a következménye annak, ha a feldolgozó megszegi az Infotv elveit, pl. nem tesz eleget a biztonsági követelményeknek vagy az adatkezelő előírásainak?			
b) Van-e a feldolgozónak kártérítési kötelezettsége szerződésszegés esetén?			
Tárgy: **2: bejelentés**		Auditor:	
2.1 Bejelentés az adatvédelmi nyilvántartásba			
a) Ki a felelős az adatvédelmi nyilvántartásba való bejelentésért?			
b) Milyen mértékben türközi a bejelentés az adatkezelés aktuális jellemzőit?			
c) Milyen gyakran vizsgálják felül a bejelentett adatokat?			
d) A bejelentett cél megfelel-e a törvényesség követelményeinek és a szervezetre vonatkozó jogi előírásoknak?			
e) Bejelentettek-e minden egyes, eltérő célú adatkezelést a kezelt adatokkal együtt?			
f) Van-e olyan adatkezelésük, melyet nem bejelentésköteles?			
2.2 A bejelentés karbantartása			
a) Milyen eljárással és gyakorisággal vizsgálják felül, hogy a bejelentés megfelel-e az aktuális adatkezelésnek?			
b) Hogyan tájékoztatják a munkatársakat arról, hogy a bejelentésben foglalt adatok megfelelnek az általuk végzett feladatoknak?			
Tárgy: **3: átmeneti intézkedések**		Auditor:	
a) Megkülönböztetik-e az			

adatkezeléseket aszerint, hogy az Infotv hatályba lépése előtt vagy azt követően kezdték-e meg, s ha igen, hogyan?			
b) Hogyan gondoskodnak arról, hogy az Infotv hatályba lépése előtt megkezdett adatkezeléseik megfeleljenek a hatályos jogi rendelkezéseknek?			

N. függelék: folyamat audit ellenőrző lista

Folyamat audit ellenőrző lista:			
Szervezet:	Szervezeti egység:		Dátum:
Folyamat:		Auditor:	
Kérdés	Vizsgált dokumentumok	Tények és megállapítások	Eredmény

---