

Az adatvédelmi és adatbiztonsági szabályzat alapvető célja négy fő követelmény érvényesítése:

- a) Tartalmaznia kell az adatkezelő által lefolytatott adatkezelés(ek) leírását (minden adatkezelési cél esetén külön-külön): milyen adatot, milyen célból - ha meg lehet határozni, - mennyi ideig kezelnek, pontosan ki az adatkezelő, ha alkalmaz, milyen adatfeldolgozót. Célszerű a szabályzatot olyan részletességgel megírni, hogy az érintett személy átláthassa a személyes adatai kezelésének útját.
- b) Az adatvédelmi rendelet és a hatályos adatvédelmi törvény meghatározza, hogy milyen tájékoztatásokat kell az adatkezelőnek az érintett számára adni. A szabályzatnak tartalmaznia kell ezeket, és meg kell határozni, hogy milyen ügyrendben kell az adatigényléseket teljesíteni. Az adatvédelmi tájékoztatónak tartalmaznia kell továbbá, hogy amennyiben az érintett kifogással, panasszal kíván élni, mely szervhez, külső intézmény fordulhat.
- c) Az adatvédelmi szabályzatnak, ha szükséges, az adatkezelőn belül meg kell határozni, hogy mely szervezeti egységnek milyen adatvédelmi feladata, kötelezettsége van. Igen fontos, hogy az adatbiztonsági rendelkezések iránymutatást adjanak a kezelt adatok védelmére, és kezelésére.
- d) A szabályzatnak végezetül konkrét, az intézmény működését lekövető adatbiztonsági szabályokat kell tartalmaznia. Elvben lehetséges, hogy jelen szabályzat csak a legfontosabb adatbiztonsági szabályokat tartalmazza, és más szabályzat, vagy ügyrend azt konkretizálja. Ebben az esetben jelen szabályzat alkalmazása elsődleges, és az ebben foglalt szabályoknak elégségesnek kell lenniük a legfontosabb kérdések, iránymutatások meghatározására.

Az adatvédelmi szabályzatnak a fenti elemeket kellő mértékben le kell írnia, és a konkrét intézmény tekintetében szükséges, a rá jellemző, egyedi adatkezelésekre is ki kell terjedjen, és azt megfelelően le kell írnia, illetőleg szabályoznia kell.

A továbbiakban egy általános adatvédelmi szabályzat legfontosabb pontjait írjuk le, és bemutatjuk, hogy az egyes címeknél milyen adatokkal kell kitölteni azt. Hangsúlyozzuk, hogy a szabályzatminta általános jellegű, és minden intézménynél, annak jellege alapján kell azt véglegesíteni. Fekete színnel azokat a rendelkezéseket írtuk, melyet javasolunk véglegesen átvenni, kék színnel a magyarázó, iránymutató tájékoztatást szedtük.

..... (szervezet megnevezése)

Adatvédelmi és adatbiztonsági szabályzata

I. A szabályzat célja

Jelen szabályzat célja, hogy az (továbbiakban: Adatkezelő) kifejtett adatvédelmi garanciák által biztosítsa az adatkezelő által végzett adatkezelések átláthatóságát, jogszerűségét, és biztosítsa az adatkezelésben érintett személyek személyes adatok védelméhez való jogát, és ezen keresztül magánszférájuk és háborítatlan szabad vallásgyakorlásukhoz való jogukat.

II. Jelen szabályzat kapcsolata más jogi normákkal

Jelen szabályzat alkalmazása során elsődleges jogforrás a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2012. évi CXII. törvény.

Az Adatkezelő adatkezelését szabályozó más belső normák jelen szabályzatnak megfelelően fogadhatók el, illetőleg módosíthatók. Amennyiben jelen szabályzat hatálybalépésekor szükséges, az adatkezelésekre vonatkozó további belső szabályzatokat felül kell vizsgálni.

III. Az érintettek köre, az adatkezelés céljai, és a célok szerint kezelt személyes adatok köre és formái, az adatkezelés formái és időtartama

Az Adatkezelő által folytatott adatkezelésben érintett személyek:

E pont alatt az adatkezelő feladatkörének ellátásához szükséges adatkezelésekben érintett személyek körét (például: iskolák esetében diákok, üdülők esetében: vendégek) kell leírni. Ettől elkülönítve kell ismertetni az intézmény működtetésével kapcsolatos adatkezelések érintettjeit (például a tisztviselők, oktatók, munkavállalók stb.), illetőleg a gazdasági működéssel kapcsolatos adatkezelések érintettjeit (ha ilyen személy van).

Az Egyházkerület által folytatott adatkezelések célja

Az adatkezelési céljának azt kell tekinteni, aminek az érvényesítése céljából a személyes adatokat gyűjtik, és kezelik. Minden egyes célt jelen pont alatt önállóan fel kell sorolni. Igen lényeges, hogy a lista teljes legyen. Adatkezelés célokat alapvetően két csoportra oszthatjuk, az intézmény szakmai feladatainak érvényesítése végett meghatározott célok (pl. oktatás), másrészt a gazdasági tevékenységgel kapcsolatos célok (pl. munkáltatás, üzemeltetés stb.)

Az Egyházkerület által vezetett adatok köre és az adatkezelés formája

- a) ...
- b) ...

Az adatok körét az adatkezelés céljaiként kell meghatározni, és kellő részletességgel leírni. A hatályos magyar jog nem követeli meg, hogy az ismertetés teljesen lefedje a kezelt adatokat, de amennyiben lehetséges, erre törekedni kell, és érvényesíteni kell azt az elvet, hogy az érintett ezen keresztül átláthassa az adatkezelést.

Az egyes adatkörök a következő időtartamig kezelhetők:

- a) ...
- b) ...

Amennyiben lehetséges, az adatköröknél meg kell határozni az adatkezelés időtartamát. Ez történhet az adatkezelésre vonatkozó jogszabályi rendelkezésre hivatkozva, illetőleg az adatkezelés időtartalmának években történő meghatározásában.

IV. A kezelt adatok jellege, az adattovábbításra vonatkozó korlátozások

Az egyes személyes adatok egyes típusai az érintett magánszféráját kevésbé, mások jóval inkább érinthetik. A hatályos adatvédelmi törvény, és az Adatvédelmi Rendelet is taxatív meghatározza azon adatok körét, melyek az érintett személyiségét érzékenyebben érintik, és ezeket szenzitív személyes adatoknak nevezi. Ilyen adatok kezelésének más a jogalapja, kezelésükre szigorúbb szabályok vonatkoznak, illetőleg az ilyen adatokkal történő visszaélésre szigorúbb szankciót határoz meg a jog.

Adatvédelmi Rendelet 9. § (1) bek. értelmében például: „A (...) vallási vagy világnézeti meggyőződésre (...) utaló személyes adatok” különleges személyes adatok. Amennyiben ilyen adatot kezel az Adatkezelő, ezen adatok körét a fenti szakaszokban elkülönülten kell meghatározni, és kezelésüknél a szigorúbb adatvédelmi szabályokra kell figyelemmel lenni. Jelen pontban az ilyen adatokra plusz garanciális szabályokat érdemes megfogalmazni.

VI. Az adatkezelő személye, és az adatvédelmi tisztviselőre vonatkozó rendelkezések

Az Adatkezelő által végzett személyes adatok kezeléséért az Adatkezelő (ügyvezető, igazgató stb.) a felelős.

A konkrét személyes adatok kezelésével kapcsolatos eljárási rendet és az adatkezelésben részt vevő tisztviselők, dolgozók kötelezettségeit jelen szabályzatban is meg lehet határozni, de önálló szabályt is lehet például ügyrendekben meghatározni. Lényeges, hogy amennyiben önálló szabályzatban végzik el a szabályozást, annak tekintettel kell lennie az adatvédelmi jogszabályokra, és jelen szabályzatra.

Az Adatkezelő valamennyi tisztségviselőjének, illetőleg az adatokhoz jogszerűen hozzáférő tagjának kötelessége, hogy az általa megismert, kezelt adatokhoz arra fel nem hatalmazott személy ne férhessen hozzá.

Az Adatkezelő vezetőségének címe, elérhetősége: ...

Az adatok megadásának a célja, hogy az érintett tudja, pontosan kihez, milyen úton tud fordulni személyes adatainak kezelésével kapcsolatos kérdésével, kifogásával.

Az Adatkezelőnek, amennyiben szenzitív adatot kezel, adatvédelmi tisztviselőt kell kineveznie. A tisztviselő az Adatkezelő vezetőjének felel, és ellátja a vonatkozó jogszabályokban foglalt feladatait. Adatvédelmi tisztviselőnek az Adatkezelő olyan munkatársa nevezhető ki, aki rendelkezik mindazon szakmai gyakorlattal és tudással, mely e feladat ellátásához szükséges. Amennyiben ilyen munkatársa nincs, megbízhatja az Magyarországi Evangélikus Egyház Országos Irodájának (a továbbiakban: Országos Iroda) adatvédelmi tisztviselőjét a feladatok ellátására.

Az adatkezelőnek abban az esetben kötelező adatvédelmi tisztviselőt kineveznie, ha a szenzitív adatok kezelése a „főtevékenységéhez” kapcsolódik. Azt, hogy mi nevezhető főtevékenységnek konkrét tevékenységi körönként lehet megítélni. Amennyiben kérdéses,

hogy a kötelezettség az adatkezelőre kiterjed, érdemes az adatvédelmi tisztviselő kinevezése mellett dönteni. Ha ilyen képzettséggel rendelkező személy az adatkezelőnél nincs, az Országos Iroda adatvédelmi tisztviselőjét érdemes megbízni.

Amennyiben az Adatkezelő új adatkezelési technológiát, eljárási rendet vezet be, adatvédelmi hatásvizsgálatot szükséges végezni annak vizsgálata céljából, hogy az újítás megfelelően biztosítja-e az adatkezelésben érintett személyek jogainak védelmét.

Fontos adatvédelmi újítása az adatvédelmi rendeletnek, hogy bevezeti az adatvédelmi hatásvizsgálatot. Ezt a kötelező esetekben el kell végezni:

- a) valószínűsíthetően magas kockázattal jár a természetes személyek jogaira,
- b) különleges személyes adatok kezelését érinti, illetőleg
- c) nyilvános helyek nagymértékű, módszeres megfigyelése (kamera-rendszerek alkalmazása) esetében.

Az adatvédelmi hatásvizsgálat szabályai jelenleg még nem kiforrottak. E mellett azonban annak elmaradása a Nemzeti Adatvédelmi és Információszabadság Hatóság oldaláról szankcionálható.

X. Az érintettek jogai

Az alábbi rendelkezések az érintett személyek számára tájékoztatást tartalmaznak, hogy hogyan, milyen módon tudják az adatkezeléssel kapcsolatos jogukat érvényesíteni. Javasoljuk változatlan formában elfogadni. Amennyiben az intézmény működése, vagy jellege okán szükséges, a szabályok konkretizálhatók, illetőleg részletezhetők azzal, hogy az érintettek jogait az alábbi szabályok korlátozásával, szigorításával nem lehet

Az Adatkezelő által kezelt adatok elsődleges forrása az érintett személy. Harmadik személytől csak akkor kérhető adat,

- a) ha azt törvény lehetővé teszi,
- b) az érintett ahhoz kifejezetten hozzájárult, illetőleg
- c) ha az adatkezelésben érintett személy 16. életévét még nem töltötte be és az adatkezeléshez a törvényes képviselő adja a hozzájárulást.

Az adatkezelésben érintett személyek saját adataikról tájékoztatást kérhetnek. A tájékoztatást indokolatlan késedelem nélkül, de legfeljebb egy hónapon belül kell az érintett részére megadni. A tájékoztatást az érintett számára az általa kért formában – szóban, írásban, a kezelt adatokról készült másolat útján, vagy elektronikusan kell megadni. A tájékoztatás megadása ingyenes.

Az érintett személy jogosult arra, hogy a következő információkról tájékoztatást kapjon az Adatkezelőtől:

- a) az adatkezelés céljáról,
- b) amennyiben lehetséges, a személyes adatok tárolásának időpontjáról,
- c) a helyesbítés és amennyiben lehetséges a személyes adatok törlésének lehetőségéről és formájáról,
- d) amennyiben adatfeldolgozót vettek igénybe, annak személyéről,

- e) ha a személyes adatait továbbították, mely személyek részére történt és milyen joggalappal,
- f) ha adatvédelmi incidens történt, annak körülményeiről, hatásáról, az elhárításra tett intézkedésekről,
- g) arról, hogy esetleges panaszával mely hatósághoz nyújthat be panaszt, illetőleg
- h) amennyiben az adatokat nem az érintettől gyűjtötték, az adatok forrásáról minden elérhető információról.

A fenti felsorolás e) pontjában foglalt panasszal az érintett döntésétől függően fordulhat:

- a) [amennyiben van, az Adatkezelő adatvédelmi tisztviselőjéhez, ennek hiányában, az Adatkezelő vezetőjéhez,](#)
- b) a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, valamint
- c) az érintett lakóhelye szerint illetékes törvényszékhez.

Ha az érintett észleli, hogy a kezelt személyes adata hibás, helyesbítését kérheti az Egyházkerület elnökségétől. Az érintett kérését, amennyiben az szükséges, indokolatlan késedelem nélkül át kell vezetni. A kérés elbírálásáig a személyes adatok kezelését korlátozni kell.

Amennyiben az érintett úgy látja, hogy a személyes adatok kezelése jogellenes, kérheti személyes adatainak törlését.

Törlés helyett zárolni kell azokat a személyes adatokat, amelyek kezelésének megszüntetése az érintett személyi jogait sérti.

Az érintett kérésének elbírálásáig a személyes adatok kezelését korlátozni kell.

Amennyiben a személyes adatok kezelését korlátozni kell, azokat felhasználni csak az érintett személy hozzájárulásával lehet.

XI. Adatbiztonságra vonatkozó szabályok

[Az adatvédelmi és adatbiztonsági szabályzat lényeges része a jelen fejezet, mely az adatbiztonsággal kapcsolatos rendelkezéseket tartalmazza. Ebben az Adatkezelőnek konkrét szabályokat kell hoznia arra, hogy milyen technikai és eljárási garanciákat alkalmaz annak érdekében, hogy a személyes adatok integritásukat megőrizzék, és jogosulatlan személy ne ismerhesse meg azokat.](#)

[A technikai intézkedések olyan szabályokat jelentenek, amelyek fizikailag biztosítják a személyes adatok védelmét. Ilyen a zárt helyiségben történő elhelyezése az adattárolónak, az adattároló számítógép jelszóval történő ellátása, szükség esetén az adattároló helyiségének klimatizálása, vagy tűzjelző berendezés elhelyezése.](#)

[Lényeges adatbiztonsági szabály, hogy a leginkább biztonságos és megfelelő technológiát kell alkalmazni. A papíralapú nyilvántartások sérülékenyek, és azok megsemmisülése, vagy elvesztése esetén a kezelt adatok nem rekonstruálhatók. Ezért, amennyiben ez anyagilag nem lehetetlen, digitalizálni kell a nyilvántartásokat, és megfelelő biztonsági intézkedések mellett meghatározott időszakonként másolatot kell készíteni az adatokról. A másolatra azonos biztonsági követelmények vonatkoznak, mint az elsődleges adathordozóra.](#)

[Szervezési intézkedések elsősorban azt jelenik, hogy az adatvédelmi szabályzatnak meg kell határoznia azt az ügyrendet, hogy kik és milyen eljárás mellett férhetnek az adatokhoz,](#)

illetőleg amennyiben az adatkezelőhöz külső intézményből adatigénylés érkezik, azt milyen protokoll szerint kell elbírálni és megválaszolni.

A továbbiakban a legfontosabb és legáltalánosabb adatbiztonsági szabályokat írjuk le azzal, hogy az adatkezelőnek a konkrét gyakorlatát kell a szabályzatban rögzítenie.

21. § (1) Az Adatkezelő az általa kezelt személyes adatokat, azok szenzitív jellegére tekintettel megfelelő technikai és szervezési intézkedések érvényesítésével kell védelemben részesíteni.

(2) A technikai intézkedések során a következő követelményeket kell érvényesíteni:

- a) biztosítani kell, hogy az adatok – papír alapú, vagy digitális – hordozója megfelelő védelemben részesüljön. Így papír alapú nyilvántartás esetén, a papírokat elzárt helyiségben, zárható szekrényben kell elhelyezni. Digitális nyilvántartás esetén a számítógépet megfelelő jelszóval kell ellátni, és amennyiben lehetséges, a számítógépet nem lehet összekötni az internettel.
- b) Fokozottan kell felügyelni, hogy a kezelt adatok ne vesszenek el, vagy jogellenesen ne módosuljanak.
- c) Kiemelten biztosítani kell, hogy a kezelt személyes adatok ne kerülhessenek arra fel nem jogosított személy(ek) birtokába.
- d) Biztosítani kell, hogy amennyiben az eredeti adathordozó megsérül, az adatok eredeti tartalmukban rekonstruálhatóak legyenek. Így digitális nyilvántartás esetén a nyilvántartásról heti vagy havi rendszerességgel kell másolatot készíteni.

(3) Szervezési intézkedéseken keresztül biztosítani kell, hogy az adatokhoz az Egyházkerület tisztviselői és dolgozói közül is csak az arra jogosult személy férhessen hozzá.

Amennyiben külső személy kér személyes adatot az Adatkezelőtől és az adatokat közvetlenül az azokat igénylő személynek továbbítanák, előtte meg kell győződni arról, hogy az adatok kezelésére valóban jogosult. Így az adatigénylését írásban kell megkérni, és abban az adatigénylés célját és jogalapját közérthető formában ki kell fejtenie. Ezt a követelményt állami szervek esetén is fokozottan érvényesíteni kell. Amennyiben kétség merülne fel az adatigénylés jogszerűségéről, azt meg kell tagadni.

Amennyiben az adatbiztonsági követelmények sérelmével a kezelt személyes adatok sérültek, megsemmisültek, elvesztek, megváltoztak, vagy jogosulatlan személy ahhoz hozzáfért, adatvédelmi incidens történt.

Ha az adatvédelmi incidens nem jelent magas kockázatot az érintett jogaira nézve, a megtörtént eseményt nyilván kell tartania. Ennek keretében rögzíteni kell a keletkezett eseményt, és a megtett intézkedéseket.

Amennyiben az adatvédelmi incidens magas kockázattal járt az érintett személy jogaira nézve, annak tudomására jutásától számított 72 órán belül be kell jelenteni a Nemzeti Adatvédelmi és Információszabadság Hatósághoz. A bejelentés tartalmi követelményeit az Adatvédelmi rendelet 33. cikke és a nemzeti jogszabályok rendezik.

XII. Záró rendelkezések

Jelen szabályzat az elfogadása napján lép hatályba. A szabályzat a helyben szokásos módon kerül közzétételre.

Kelt: 2018.