II. Fejezet

Jelen fejezet az Adatvédelmi és adatbiztonsági szabályzat szerves és elválaszthatatlan része!

Információbiztonsággal kapcsolatos adatkezelések

1. Az adatvédelmi incidens

1

1.1. Az incidens bejelentése:

Az a munkavállaló, aki a Hivatal által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést észlel, azt köteles a közvetlen vezetőjének haladéktalanul bejelenteni, megadva a nevét, telefonszámát és/vagy e-mail címét, a szervezeti egységét, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e. A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

A vezető a bejelentést követően tájékoztatja az adatvédelemre kijelölt személyt az adatvédelmi incidens bekövetkezéséről, megadva a bejelentő nevét, telefonszámát és/vagy e-mail címét, szervezeti egységét, továbbá a bejelentett adatvédelmi incidens tárgyát, azt, hogy az incidens informatikai rendszert érint-e, valamint a további, a bejelentő által tudomására hozott egyéb információkat.

Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, akkor a vezető az informatikai szervezetet is tájékoztatja.

Amennyiben a Hivatal ellenőrzésre jogosult szervezeti egységei a feladataik ellátása során adatvédelmi incidenst észlelnek, az adatvédelemre kijelölt személyt értesítik. Ezen személy a bejelentések értékelését követően:

- a bejelentés megvizsgálása és az incidens kezelése,
- ő – informatikai rendszert érintő incidens esetén az informatikai szervezettel együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 2 munkanapon belül teljesíteni.

Az adatszolgáltatásnak tartalmaznia kell:

a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit, hatásait,
c) az incidens során kompromittálódott adatok körét, számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedések leírását,
f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens vizsgálatot igényel, annak végrehajtására az adatvédelemre kijelölt személy felkéri a Vezetőséget, informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az informatikai szervezetet is bevonva. Jelen személy szaktanácsadóként közreműködik a vizsgálat lefolytatásában.

Az adatszolgáltatás alapján és az adatvédelemre kijelölt személy – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az informatikai szervezettel együtt – javaslatot tesz az adatvédelmi incidens elhárításához szükséges intézkedésekről az adatok kezelését vagy feldolgozását végző szakterületnek.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében – az Információ Biztonsági Szabályzat alapján kijelölt adatgazda egyetértésével dönt.
Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, kijelölt adatgazda esetében az adatgazda az adott intézkedések végrehajtását minél hamarabb köteles az adatvédelemre kijelölt személyt tájékoztatni.

1.2. Az incidens nyilvántartása

Az adatvédelmi incidensről a adatvédelemre kijelölt személy nyilvántartást vezet.

A nyilvántartásba rögzíteni kell:

a) az érintett személyes adatok körét,
b) az adatvédelmi incidenssel érintettek körét és számát,
c) az adatvédelmi incidens időpontját,
d) az adatvédelmi incidens körülményeit, hatásait, az adatvédelmi incidens elhárítására megtett intézkedéseket,
e) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az adatvédelemre kijelölt személy megőrizni.

Jelen Szabályzat 19. sz. melléklete incidensnyilvántartó mintát tartalmaz.

2. Hatásvizsgálat

2.1. Az adatvédelmi hatásvizsgálat célja

A GDPR 24. cikk (1) bekezdése úgy rendelkezik, hogy *„Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a Rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi."*

A GDPR fenti bekezdése tehát a Hivatalt arra kötelezi, hogy a rendelkezések betartásának biztosítása érdekében megfelelő intézkedéseket tegyen. Ez azt jelenti, hogy a természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben a Hivatalnak fel kell mérnie a kockázat valószínűségét és súlyosságát.

Erre szolgál az adatvédelmi hatásvizsgálat, amely magában foglalja az említett kockázat mérséklését, a személyes adatok védelmét, valamint a GDPR-nek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat. Vagyis az adatvédelmi hatásvizsgálat egyfajta alátámasztása annak, hogy a személyes adatok kezelése a szabályoknak megfelelően történik.

Az adatvédelmi hatásvizsgálat célja tehát alapvetően a természetes személyek jogait és szabadságait érintő kockázatok megfelelő kezelésének elősegítése, amelyhez legfőképp az alábbiak feltárása szükséges:

a) az adatkezelés jellegének meghatározása;
b) az adatkezelési műveletek szükségességének és arányosságának vizsgálata;
c) annak feltárása, hogy milyen kockázatokkal lehet számolni és azok kezelésére milyen intézkedések szolgálhatnak.

A GDPR 35. cikke alapján adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

a) amikor a személyes adatkezelés célja a természetes személyekkel kapcsolatos döntés meghozatala, méghozzá a természetes személyek személyes jellemzőinek szisztematikus, kiterjedt és automatizált értékelése alapján (pl.: profilalkotás);
b) a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, mint a személyes adatok különleges kategóriáinak kezelése;
c) a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy
d) nyilvános helyek nagymértékű, módszeres megfigyelése, különösen abban az esetben, ha azt elektronikus optikai eszközök alkalmazásával hajtják végre;
e) ha az illetékes felügyeleti hatóság úgy ítéli meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, különösen mivel megakadályozza, hogy az érintettek a jogaikat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, illetve szerződést érvényesítsenek, esetleg mindössze azért, mert az említett műveletekre szisztematikusan és nagy számban kerül sor.

A gyakorlatban ez azt jelenti, hogy a Hivatalnak folyamatosan értékelnie kell az adatkezelési tevékenységeiből eredő kockázatokat, hogy felismerje, ha az adatkezelés valamely fajtája valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Ezt a GDPR 35. cikkének (11) bekezdése is alátámasztja, amely szerint *„Az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e”.*

A Hivatal jelen Szabályzat 20. sz. mellékletében leírt szempontrendszer figyelembevételével elvégzi a hatásvizsgálatot.

3. Érdekmérlegelés

Az GDPR rendelkezései szerint lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy az Adatkezelő eleget tesz tájékoztatási kötelezettségének. Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a)-f) pontjai az irányadók.

Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat, akkor és annyiban lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

Az adatkezelés jogszerűségének vizsgálatához a Hivatal elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az érdekmérlegelési teszt során a Hivatal azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. Az egymással ellentétes jogok és érdekek súlyozásának feltételét mindig az adott eset sajátos körülményeire való tekintettel vizsgálja a Hivatal. A Hivatal a mérlegelés során figyelembe veszi különösen a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát, stb.

Az érdekmérlegelési teszt részeként a szükségesség és arányosság vizsgálatát is elvégzi a Hivatal, amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján a Hivatal megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, hogy a Hivatal az érintett beleegyezése nélkül kezeli a személyes adatot, tehát a Hivatal adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait. A Hivatal tájékoztatja az érintetteket a hozzájárulás hiányára tekintettel alkalmazott adatvédelmi garanciákról és az adatkezelés elleni tiltakozás lehetőségeiről.

Nem írható elő az ellentétes érdekek és jogok közötti súlyozás eredménye anélkül, hogy eltérő eredményt tenne lehetővé a Hivatal az adott eset sajátos körülményeire tekintettel, ezért a Hivatal minden egyes esetben külön érdekmérlegelési tesztet végez el.

Lehetséges forgatókönyv, amelytől való eltérés jogát a Hivatal fenntartja:

a) a Hivatal a tervezett adatkezelés megkezdése előtt áttekinti, hogy a célja elérése érdekében feltétlenül szükséges-e személyes adat kezelése: rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával személyes adatok kezelése nélkül megvalósítható a tervezett cél;
b) a Hivatal a jogos érdekét a lehető legpontosabban meghatározza;
c) a Hivatal meghatározza, hogy mi az adatkezelés célja, milyen személyes adatok, meddig tartó adatkezelését igényli a jogos érdek;
d) a Hivatal meghatározza, hogy az érintetteknek mik lehetnek az érdekeik az adott adatkezelés vonatkozásában (pl.: azok a szempontok, amelyeket az érintettek felhozhatnának az adatkezeléssel szemben);
e) a Hivatal elvégzi jogos érdekeinek és az érintettek érdekeinek, alapjogainak súlyozását és ez alapján megállapítja, hogy a személyes adat kezelhető-e. A Hivatal meghatározza, hogy miért korlátozza arányosan a Hivatal jogos érdeke – és az ennek alapján végzett adatkezelés – a 4. lépésben meghatározott érdekelti jogokat, várakozásokat;
f) a Hivatal meghatározza, mely garanciák biztosíthatják az adatkezelés szükségességét-arányosságát (természetesen más garanciális intézkedések is alkalmazhatók).

A Hivatal jelen Szabályzat 15. sz. mellékletében leírt szempontrendszer figyelembevételével végzi el az érdekmérlegelést.

4. Adatbiztonság

A GDPR 32. cikke kimondja, hogy az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatókörei, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a

kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve – többek között – adott esetben:

a) a személyes adatok álnevesítését és titkosítását,

b) a személyes adatok kezelésére használt rendszerek folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét,

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen álltani,

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedéseknek hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

4.1. Az információbiztonságnak három kiemelt célja van:

1) a bizalmasság (confidentiality),
2) a sérthetetlenség (integrity),
3) a rendelkezésre állás (availability).

Ez az úgynevezett CIA-háromszög. Ezen belül szintén három kontrollt különböztetünk meg:

- fizikai,
- logikai,
- adminisztratív kontroll.

4.2. Fizikai kontroll

A számítógépes környezethez való hozzáférés korlátozása, valamint az adatmentés biztosítása.

4.3. Adminisztratív kontroll

A Hivatalnak belső szabályai, rendelkezései, eljárás rendjei tartoznak ezen kontroll alá. Az Adatkezelőnek rendelkeznie szükséges egy üzletmenet-folytonossági tervvel, valamint egy katasztrófaelhárítási tervvel.

4.4. Logikai kontroll

Olyan intézkedések, mint például a jelszó- és erőforrás- menedzsment, azonosság- és jogosultságkezelés, logikai hozzáférés, információbiztonsági eszközök, illetve hálózati konfiguráció.

5. Adatbiztonság

A Hivatal több saját szerverrel rendelkezik, amelyek a székhelyen találhatóak.

A papíralapon kezelt személyes adatok biztonsága érdekében az Adatkezelő, összhangban a hatályos iratkezelési szabályokat rögzítő Szabályzat előírásaival, az alábbi intézkedéseket alkalmazza:
az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
az Adatkezelő adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rábízott adathordozókat elzárja, vagy az irodát bezárja;
az Adatkezelő adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az Adatkezelő.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az Adatkezelő, összhangban a hatályos Információbiztonsági szabályzatának előírásaival, az alábbi intézkedéseket és garanciális elemeket alkalmazza:
az adatkezelés során használt számítógépek az Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír a Adatkezelő;
a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről Adatkezelő rendszeresen, illetve indokolt esetben gondoskodik;
az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el az Adatkezelő az adatvesztést;
a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik, és mágneses adathordozóra történik;
a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolt;
a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

A honlapra feltöltendő tájékoztató a Szabályzat 17. sz. melléklete.

Ezen szabályokat az *Információ Biztonság Szabályzat is* tartalmazza.

A BYOD tiltott szintén az *IBSZ* része.

Az internet hozzáférést is szabályozott.

A céges eszközökön csak a Hivatal rendelkezik admin joggal, így az alkalmazások telepítése ellenőrzött, a felhasználó által nem lehetséges. A magánjellegű file-ok tárolása nem megengedett.

5.1. Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészsége nagymértékben hozzásegíti a Hivatalt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.
A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre.

5.2. Jogosultságkezelési folyamat

Jogosultságigényléshez, módosításhoz jogosultságkezelési megrendelőlapot kell küldeni. A megrendelőlapot papíralapon vagy elektronikus formátumban, az aláírt példányt beszkennelve kell eljuttatni az informatikusnak. A jogosultságot a megbízott, harmadik partner állítja be.

Az informatikus minden esetben konzultál az megrendelőlapon szereplő jogosultság megadásáról vagy módosításáról annak indokoltságának tekintetében a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezérigazgatónak Jegyzőnek van.