DPIA-információ

DPIA
A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény (Dáptv.) tervezetével kapcsolatos adatvédelmi hatásvizsgálat

Készítő szervezet
Miniszterelnöki Kabinetiroda

Létrehozás dátuma
13/10/2023

Összegzés

A hatásvizsgálat célja

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 25/G. § (6) bekezdésében meghatározott adatvédelmi hatásvizsgálat elvégzése, ennek keretében a tervezett új kötelező adatkezelések áttekintése és kockázatelemzése. Az Infotv. hivatkozott rendelkezése szerint a kötelező adatkezelést előíró jogszabály előkészítője az Infotv. 25/G. § (5) bekezdése szerinti tartalommal adatvédelmi hatásvizsgálatot folytat le.

A kötelező adatkezelések az Infotv. 5. § (3) bekezdése értelmében az Infotv. 5. § (1) bekezdés a) pontjában, a (2) bekezdés b) pontjában, valamint a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i 2016/679/EU rendelet (általános adatvédelmi rendelet; a továbbiakban: GDPR) 6. cikk (1) bek. e) pontjában meghatározott adatkezelések.

Az Infotv. 25/G. § (5) bekezdése szerinti kötelező adattartalom az Infotv. alapján a következő:

a) a tervezett adatkezelési műveletek általános leírása,

b) az érintettek alapvető jogainak érvényesülését fenyegető, az adatkezelő által azonosított kockázatok leírása és jellege,

c) az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedések.A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény tervezete (a továbbiakban: Dáptv.) a digitális szolgáltatás nyújtásához szükséges adatkezeléseket részletesen nem szabályozza, és a Kormánynak ad felhatalmazást arra, hogy azokat a későbbiekben rendeletben szabályozza, ennek megfelelően a jogalkotás jelen szakaszában még az adatkezelésből eredő konkrét kockázatok nem azonosíthatóak be. Erre figyelemmel a jelen hatásvizsgálatnak nem lehet célja az adatkezelések, az adatkezelési folyamatok teljes körű leírása. A Nemzeti Adatvédelmi és Információszabadság Hatóság

tájékoztatásának megfelelően [lásd: Jogszabálytervezetek adatvédelmi hatásvizsgálata - Nemzeti Adatvédelmi és Információszabadság Hatóság (naih.hu)] – jelen hatásvizsgálati dokumentációban e körülmény egyértelműen jelzésre került, és a jelen hatásvizsgálat kiegészítésére az adatkezelés részletes szabályainak kiadását követően a jövőben várhatóan sor kerül.

Az adatvédelmi hatásvizsgálat tárgyát képező adatkezelések

A Dáptv. az alábbi, a természetes személyek jogaira és szabadságaira a hatályos, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényhez (a továbbiakban: E-ügyintézési tv.) képest lényegi változást jelentő intézkedéseket szabályozná, ezért jelen hatásvizsgálat az alábbiakra terjed ki:

1. digitális állampolgár azonosító (a továbbiakban: DÁP azonosító), amit a digitális állampolgárság nyilvántartást vezető szerv generál és tart nyilván;
2. a digitális állampolgárság szolgáltató által biztosításra kerülő, elsődlegesen mobil eszközökre fejlesztett digitális szolgáltatások igénybevételéhez szükséges keretalkalmazás és keretszolgáltatások, mely utóbbiak igénybevételéhez a felhasználó regisztrációja és a mobilalkalmazás mobileszközre történő letöltése szükséges;
3. a digitális szolgáltatást biztosító szervek köre, ezáltal a személyes adatokon – adatkezelőként vagy adatfeldolgozóként – adatkezelési műveleteket végző szervezetek köre bővül;
4. életesemény szolgáltató által végzett adatkezelési műveletek.

A hatékony, eredményes ügyintézés érdekében és elsősorban az életesemény-alapú fejlesztések megvalósítása és szolgáltatások nyújtása érdekében a digitális állampolgárság szolgáltató, illetve az adott digitális szolgáltatás nyújtója általános adatkezelési felhatalmazást kap az ügycsoport integrált intézéséhez. A digitális állampolgárság szolgáltató ennek érdekében, a nyilvántartások közötti kapcsolatokat felhasználva hozzáférhet az ügy elintézéséhez szükséges személyes adathoz és azokat kezelheti. Az egyes életesemények megoldásához, az ezekhez kapcsolódó ügyintézéshez szükséges összesített adatköröket kormányrendelet sorolja fel törvényi felhatalmazás alapján. A rendeleti

szintű felhatalmazás indoka alapvetően az, hogy a rendeleti szintű szabályozás kiterjedtsége elősegíti a rugalmas alkalmazkodást a technológiai és szolgáltatásbeli változásokhoz, fejlesztésekhez.

Adatkezelők

A digitális állampolgárság nyilvántartás tekintetében az adatkezelő a Kormány rendeletében kerül kijelölésre.

A keretalkalmazás és a keretszolgáltatások tekintetében a digitális állampolgárság szolgáltató az adatkezelő.

A digitális szolgáltatások nyújtásával összefüggésben adatkezelők még a digitális szolgáltatást biztosító szervezetek.

Az egyes életesemények vonatkozásában az életesemény szolgáltató és a szakmai közreműködők a Kormány rendeletében kerülnek kijelölésre.

Adatok, az adatkezelés jellege, az adatkezelési műveletek általános leírása

Általános megállapítások

Általánosan rögzíthető, hogy a Dáptv. alapján automatizált döntéshozatal, vagy profilalkotás nem valósul meg. A törvény tartalmazza az automatizált döntéshozatal általános, a GDPR-hez kapcsolódóan kiegészítő szabályait, maga a törvény azonban nem hoz létre ilyen tevékenységet. Amennyiben valamely szervezet a törvény alapján automatizált döntéshozatal bevezetését határozza el, úgy az adatkezelő köteles az ezzel kapcsolatos elemzések elvégzésére.

Önmagában a Dáptv. alapján továbbá nem történik különleges személyes adatok kezelése. Olyan szervezetek is a törvény hatálya alá tartoznak, amelyek különleges személyes adatokat kezelnek, azonban az ezzel kapcsolatos kockázatelemzést és hatásvizsgálatot az érintett szervezetek az általuk végzett adatkezelés tekintetében kötelesek elkészíteni.

Az új technológiák alkalmazása körében rögzíthető, hogy az adatkezelés megvalósítását végző technológiák mind már létező, a piacon elérhető szolgáltatások. A Dáptv. alapján új technológia kifejlesztésére nem került sor. Habár az ügyintézés tekintetében a mobil alapú ügyintézés elsődlegessége jelentős előrelépés, maga a technológia bevettnek és már a közigazgatásban is alkalmazottnak tekinthető.

Az adatkezelés nagyszámú állampolgárt érint, de az állampolgárokra vonatkozó adatkezelésre csak a szükséges mértékben kerül sor, a kötelező adatkezelés (így pl. a digitális állampolgárság nyilvántartás) csak a szükséges minimális adatokra korlátozott nyilvántartás. Minden más, az ügyfelet érintő adat kezelése csak ideiglenesen történik, ide nem értve az egyes hatósági ügyeket intéző eljárásokhoz kapcsolódó (az adott ágazati jogszabály által szabályozott) adatkezeléseket.

Az egyes adatkezelések elemzése

A Dáptv. alapvetően az E-ügyintézési tv. szerinti adatkezelési modellt veszi át, azt fejleszti tovább, erre tekintettel a jelen adatvédelmi hatásvizsgálat keretében kizárólag az attól való eltérések kerülnek bemutatásra.

1. Digitális állampolgár azonosító és digitális állampolgárság nyilvántartás

A DÁP azonosító egy olyan – matematikai módszerrel képzett, különleges adatra nem utaló – számjegysor, amely egyedi és tartós azonosítóként a polgárt a digitális térben egyértelműen azonosítja.

A DÁP azonosító célja egységes hozzáférés biztosítása a digitális térben való ügyintézéshez, vagyis az, hogy a digitális tér nyújtotta szolgáltatásokhoz egy általánosan használható azonosítóval lehessen hozzáférni.

A digitális szolgáltatásokhoz szükséges - egyes nyilvántartásokban vagy szerveknél elérhető - adat vagy irat automatizált rendelkezésre állása is a DÁP azonosító használatával lehetséges.
A DÁP azonosítón alapuló felhasználói profil szolgál az állammal való elsődleges kapcsolattartásra.

Mindez hozzájárul a digitális szolgáltatások felhasználóbarát és ügyfélközpontú nyújtásához, egyben lehetővé teszi, hogy a digitális szolgáltatások hatékonyan és magas színvonalon működhessenek.

Jelenleg az ágazati azonosítók mellett a természetes azonosító adatok (viselt név, születési név, születési hely és idő, valamint az anyja neve; a továbbiakban együtt: 4T adatok) alapján történik az azonosítás, ezért az érintettnek ezeket – az érdemi ügyintézés szempontjából irreleváns – adatokat mindig meg kell adnia, melyek kezelésére az állami – és gyakran a nem állami – nyilvántartások vezetői jogszabály alapján jogosultak.

A természetes azonosító adatokhoz képest a DÁP azonosító egy önmagában értelmetlen számsor, így annak használata a természetes személyek jogaira és szabadságaira nézve kevésbé kockázatos,

mint a 4T adatok megadása.

A GDPR 87. cikke értelmében – az érintettek jogait és szabadságait védő megfelelő garanciák biztosításával – lehet kezelni általános jellegű azonosítókat.

„A tagállamok részletesebben meghatározhatják a nemzeti azonosító számok vagy egyéb általános jellegű azonosító jelek kezelésének konkrét feltételeit. Ebben az esetben a nemzeti azonosító számok, illetve az egyéb általános jellegű azonosító jelek felhasználására *kizárólag az érintett jogainak és szabadságainak e rendelet szerinti megfelelő garanciái mellett kerülhet sor*."

A DÁP azonosítót a digitális állampolgárság nyilvántartást vezető szerv generálja és tartja nyilván.

A digitális állampolgárság nyilvántartás a jelenlegi központi ügyfélregisztrációs nyilvántartásra (a továbbiakban: KÜNY) épül. A KÜNY adattartalma egészül ki a DÁP azonosítóval, valamint azzal a ténnyel, hogy az állampolgár nyilatkozott-e arról, hogy a jövőben digitális állampolgár kíván-e lenni („felhasználói profil aktiválása") vagy korábbi nyilatkozatát vissza kívánja vonni („felhasználói profil inaktiválása").

A digitális állampolgárság nyilvántartást vezető szerv kezelheti az így kibővült nyilvántartásban található adatokat annak érdekében, hogy a digitális térben megjelenő digitális állampolgárok egyértelműen megfeleltethetők legyenek az érintett természetes személyekkel.

Az állampolgár kezdeményezi a felhasználói profilja aktiválását, továbbá kezdeményezheti a felhasználói profilja inaktiválását.

A digitális állampolgárrá válás tehát egyfelől nem kötelezettség, csupán lehetőség a természetes személy állampolgárok számára, amely egyszerűsíti az ügyintézés és az azonosítás folyamatát, másfelől a szükséges mértékre csökkenti az érintett azonosításához felhasznált adatait, amelyek egyébként az állami nyilvántartásokban szerepelnek.

A DÁP azonosító ismerete önmagában nem teszi lehetővé semmilyen – állami vagy nem állami –

nyilvántartásban tárolt adat megismerését. Az érintettre vonatkozó bármely adat, információ csak akkor ismerhető meg, ha arra az adatigénylőnek van felhatalmazása. A felhatalmazás jogszabályon vagy az érintett hozzájárulásán alapul, azaz a (személyes) adatok megismerésének lehetőségét ebben a tekintetben nem bővíti a DÁP azonosító bevezetése.

2. Digitális állampolgárság szolgáltató adatkezelési tevékenysége

A digitális állampolgárság szolgáltató által a digitális térben nyújtott keretszolgáltatások az eAzonosítás, az eAláírás, az ePosta, az eDokumentumkezelés, valamint az eFizetés. A digitális állampolgárság szolgáltató a felhasználó részére keretalkalmazást biztosít, mely egyenként vagy összesítetten biztosítja a digitális szolgáltatások elérését, illetve igénybevételét.

A digitális térben történő szolgáltatás-igénybevétel, valamint az ügyintézés során a digitális állampolgárság szolgáltató – a digitális szolgáltatások hatékonyságának és magas színvonalának biztosítása, az ügyintézési határidő és az ügyhöz kapcsolódó egyéb adminisztrációs terhek csökkentése és az egyidejűleg több ágazatot érintő integrált ügymenet kialakítása céljából – a felhasználó mindazon személyes adatához hozzáférhet, de csak azokat kezeli, amelyek az igénybe vett adott digitális szolgáltatás nyújtásához szükségesek. A digitális állampolgárság szolgáltató – digitális adatkezelőként – jogosult ezeket az adatokat a szolgáltatás nyújtásához szükséges és elégséges mértékben átvenni és továbbítani.

A Dáptv. felhatalmazása alapján a későbbiekben kormányrendelet határozza meg azokat a konkrét személyes adatokat, amelyek az egyes szolgáltatások nyújtásához elengedhetetlenül szükségesek, vagyis a kezelt adatok körének meghatározására a digitális állampolgárság szolgáltató nem jogosult, ezt csak a jogalkotó teheti meg, amit minden esetben megfelelő előkészítés, és mérlegelés előz meg annak érdekében, hogy valóban csak a szükséges mértékű adatkezelésre kerüljön sor.

A DÁP keretalkalmazás a felhasználó mobiltelefonján fut, ahonnan megfelelő azonosítást követően érhető el, válik hozzáférhetővé.

3. Digitális szolgáltatást biztosító szervek adatkezelési tevékenysége

A digitális szolgáltatás biztosító szervek között meg kell különböztetni a

a) digitális szolgáltatás nyújtására köteles szervet,
b) a digitális szolgáltatás biztosítására kötelezett szervezetet, valamint
c) a digitális szolgáltatás nyújtását önként vállaló jogalanyt.

A digitális szolgáltatás nyújtására köteles szervek köre alapvetően megegyezik a hatályos E-ügyintézési tv.-ben szereplő elektronikus ügyintézést biztosító szervek körével.

Digitális szolgáltatás biztosítására kötelezett szervezetnek minősül:

- a hulladékról szóló törvény szerinti hulladékgazdálkodási közszolgáltatási résztevékenység körébe tartozó szolgáltatást nyújtó,
- a távhőszolgáltatásról szóló törvény szerinti távhőszolgáltató,
- a földgáz egyetemes szolgáltatásra jogosult felhasználó részére földgáz-kereskedelmi szerződés vagy elosztóhálózat-használati szerződés alapján nyújtandó szolgáltatás nyújtó,
- a víziközmű-szolgáltatásról szóló törvény szerinti víziközmű-szolgáltatást nyújtó,
- a nem közművel összegyűjtött háztartási szennyvíz rendszeres begyűjtésére, gyűjtésére, elszállítására és elhelyezésére irányuló szolgáltatást nyújtó,
- a kéményseprő-ipari szolgáltatást nyújtó,
- az egyetemes postai szolgáltatást nyújtó,
- a villamos energia egyetemes szolgáltatásra jogosult felhasználó részére villamosenergia-vásárlási szerződés vagy hálózathasználati szerződés alapján nyújtandó szolgáltatást nyújtó,
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló törvény szerinti hitelintézet és pénzügyi szolgáltató,
- az egyes fizetési szolgáltatókról szóló törvény szerinti pénzforgalmi intézmény, elektronikuspénz-kibocsátó intézmény és a Posta Elszámoló Központot működtető

intézmény,

- a biztosítási tevékenységről szóló törvény szerinti biztosító és viszontbiztosító,
- a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló törvény szerinti befektetési vállalkozás és árutőzsdei szolgáltató,
- az Önkéntes Kölcsönös Biztosító Pénztárakról szóló törvény, a magánnyugdíjról és a magánnyugdíjpénztárakról szóló törvény, valamint a foglalkoztatói nyugdíjról és intézményeiről szóló törvény hatálya alá tartozó tevékenységet végző,
- a biztosítási tevékenységről szóló törvény szerinti biztosító egyesületi szolgáltatást nyújtó, valamint
- a tervek szerint ebbe a kategóriába fog tartozni az elektronikus hírközlésről szóló törvény szerinti, egyéni előfizetői szolgáltatást nyújtó elektronikus hírközlési szolgáltató gazdálkodó szervezet.

Ezen szervek – a hatályos normatív rendelkezések alapján – akkor férnek hozzá az érintettek személyes adataihoz, ha erre kifejezett jogszabályi felhatalmazásuk van (ilyen például a Pmt. szerinti átvilágítás) vagy ha ehhez az érintett kifejezetten hozzájárult (ma így működik például a népszerű e-bejelentő szolgáltatás).

Az adatkezelés tekintetében tehát érdemi változás nincs, a szervekre vonatkozó kötelezés – adatkezelési szempontból – annyi változást jelent, hogy képesnek kell lenniük az általuk kezelendő, kezelhető adatokat olyan csatornákon, olyan szolgáltatásokon keresztül fogadni, amelyek az érintett ügyfelek kényelmét és az adatkezelés, adattovábbítás fokozott biztonságát szolgálják.

A digitális szolgáltatás nyújtását önként vállaló jogalanyokra a fentiek vonatkoznak.

4. Az életesemény szolgáltató

Az életesemény-alapú ügyintézés keretében az ügyintézést az egyes életesemények szerint tematizált és integrált ügymenetet biztosító ügyintézési rendszerekkel kell támogatni. Az életesemény alapú ügyintézés arra épül, hogy az emberek életük során nem hatóságokkal és

ügyekkel, hanem különböző élethelyzetekkel találkoznak, például születés, házasság, munkavállalás, nyugdíjazás vagy egészségügyi problémák. Az ügyeket tehát ezen tipikus életeseményekhez kell rendezni és azokat lehetőség szerint egységes folyamatban kezelni függetlenül attól, hogy az hány szervezet milyen hatáskörébe tartozik, azt milyen típusú üggyel – vagy ügyekkel – lehet intézni. Az életesemény-alapú szolgáltatásokat a Kormány rendeletben állapítja meg, szintén ezen rendeletben kerül kijelölésre a szakmai közreműködő. A szakmai közreműködő a vonatkozó ágazati szabályozás alapján kezeli az adatokat, tehát az adatkezelésben a szakmai közreműködőt érintően változás nincs.

Az életesemény-alapú szolgáltatások kialakításának meghatározó szereplője az adott életeseményhez rendelt kijelölt szolgáltató, amelyet a Dáptv. a szükséges döntési jogokkal és adatkezelési felhatalmazással felruház.

Az életesemény-alapú szolgáltatás kialakítása és működtetése során annak szolgáltatója kialakítja az eredményes szolgáltatáshoz szükséges adatkapcsolatokat és szükséges mértékben kezel adatot, az adatkezelés minimalizálásának és célhoz kötöttségének betartásával.

Az életesemény-alapú szolgáltatásokat és annak fő adatkezelési, együttműködési szabályait kormányrendelet állapítja meg.

A Dáptv. felhatalmazása alapján a későbbiekben kormányrendelet határozza meg azokat a konkrét személyes adatokat, amelyek az egyes szolgáltatások nyújtásához elengedhetetlenül szükségesek, vagyis a kezelt adatok körének meghatározására az életesemény szolgáltató nem jogosult, ezt csak a jogalkotó teheti meg, amit minden esetben megfelelő előkészítés, és mérlegelés előz meg annak érdekében, hogy valóban csak a szükséges mértékű adatkezelésre kerüljön sor.

A személyes adatok kezelésére szolgáló alapvető eszközök és környezet

Az adatkezelés a jogszabály által kijelölésre kerülő digitális állampolgárság szolgáltató által működtetett informatikai alkalmazásban („DÁP keretalkalmazás"), valamint a digitális állampolgárság nyilvántartás vezetését támogató szakrendszerben (a továbbiakban: DÁNY) történik.

A DÁP keretalkalmazás backend-je és a DÁNY a NISZ Zrt. által üzemeltetett Kormányzati Adatközpontban kerül elhelyezésre, itt biztosíthatók a természetes személyeknek a GDPR, az Infotv. rendelkezéseinek való megfelelés, valamint az állami és önkormányzati szervek informatikai biztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) szerinti információbiztonsági követelmények teljesítése.

Megfelelés egyes alapelveknek, az arányosság és a szükségesség vizsgálata

Az adatkezelés céljai meghatározottak-e, egyértelműek-e és jogszerűek-e?

Az adatkezelés célja: a Dáptv. közpolitikai célja az állam és a társadalom kapcsolatának digitális térbe – azaz az állami, társadalmi és gazdasági interakciók személyes jelenlétet mellőző, elektronikus úton történő megvalósításának környezetébe – helyezése, a modern kormányzati digitális felületek és szolgáltatások létrehozása érdekében.

A jelen hatásvizsgálattal érintett adatkezelések elsődleges célja a természetes személyek részére hozzáférés biztosítása ezen digitális szolgáltatásokhoz, és a digitális szolgáltatások magas színvonalú, ügyfélközpontú és felhasználóbarát nyújtása.

Az adatkezelés egyértelműsége: ezzel kapcsolatban egyfelől a Dáptv., másfelől az elfogadását követően elkészülő végrehajtási rendeletek szerinti részletszabályok fogják meghatározni az egyes adatkezelési műveletek tartalmát és az adatkezelés határait, amely jogszabályokhoz kapcsolódóan, az adatkezelések megkezdését megelőzően hatásvizsgálat fog készülni.

Az adatkezelés jogszerűsége, jogalapja: az adatkezelés jogalapja és az adatkezelés módja a Dáptv.-

ben, valamint részletesen az ahhoz kapcsolódó végrehajtási rendeletekben lesz meghatározva. Az adatkezelések jogalapja ezen esetekben a GDPR 6. cikk (1) bekezdés e) pontja, mivel az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladata végrehajtásához szükséges.

A digitális állampolgár a Dáptv.-ben lehetővé tett, vagy az azon alapuló, de ott adatkezelési szempontból részletesen nem szabályozott digitális szolgáltatásokat is igénybe vehet. Ezen esetekben az adatkezelés célja egyedileg mindig konkrétan meghatározásra kerül, és az adatkezelés jogalapja ebben az esetben a GDPR 6. cikk (1) bekezdés a) pontja szerint az érintett hozzájárulása.

Jelen adatvédelmi hatásvizsgálat azokra a kötelező adatkezelésekre vonatkozik, amelyek esetében a jogalap:

- a GDPR 6. cikk (1) bekezdés e) pontja (az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges).

Szükségesség és arányosság: A digitális állampolgárság fejlesztések célja az ügyfelek, valamint a szolgáltatók (közmű- és hírközlési szolgáltatók) adminisztratív terheinek csökkentése, a hatósági és más típusú ügyintézési folyamatok fejlesztése, az állam szolgáltató jellegének erősítése. Az állampolgár ennek megfelelően nem kötelezhető a digitális térben rendelkezésre álló adat ismételt megadására.

A digitális állampolgárság szabályozása útján biztosítható, hogy az ügyfelek az egyes ügyeket az őket érintő életeseményhez rendezett módon, a lehető legegyszerűbben, integrált módon, elektronikus úton tudják elintézni, lehetőség szerint mobiltelefonról – megkímélve ezzel magukat is a hosszadalmas ügyintézési folyamatoktól, illetve a szerveket is a rendkívüli adminisztratív ügyintézéstől. A szabályozásban meghatározott mindezen célok összhangban vannak az általános adatvédelmi alapelvekkel, a szükségesség és az arányosság követelményével is.

Az adatkezelés törvényi szabályozáson alapul, meghatározva az adatkezelési tevékenységeket, amelyet az érintett szervek, szolgáltatók kezelhetnek. Az adatkezelést így a törvényben

meghatározott célok megvalósítása indokolja, ügyelve arra, hogy az arányosan, csak a legszükségesebb adatokra terjedjen ki és ügyelve arra, hogy azoknak csak a szükséges ideig történjen meg a kezelése.

A kötelező adatkezelés a valóban indokolt körre korlátozott; ahol a kötelező adatkezelés elrendelése nem indokolt (pl. proaktív szolgáltatások nyújtása), ott a szabályozás az állampolgár hozzájárulásától teszi függővé az adatkezelést.

A DÁP azonosító adatkezelője, valamint az életesemény szolgáltató a céllal arányban álló mértékben kezel az adatokat, megtéve a szükséges intézkedéseket annak érdekében, hogy az adatkezelés ne okozzon aránytalan hátrányt az érintetteknek. Az DÁP azonosító adatkezelője a garanciális szabályok rögzítése érdekében adatvédelmi szabályzatot készít, amelynek betartását folyamatosan ellenőrzi.

Jogszerűség: Az adatkezelés jogszerűségét a Dáptv. szerinti tervezett szabályozás és a GDPR 6. cikk (1) bek. e) pontja adja meg, amely értelmében „a személyes adatok kezelése (...) jogszerű, amennyiben (...) „az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges".

Átláthatóság: a Dáptv. és a végrehajtási rendeletei alapján történő adatkezelések során az adatkezelési tevékenységet végzők kiemelt figyelmet fordítanak majd arra, hogy az adatkezelés a természetes személyek számára átlátható legyen, így arra is, hogy az érintetteknek nyújtott tájékoztatás könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.

A Dáptv. alapján egyértelműen meghatározott, hogy a digitális szolgáltatásokhoz való hozzáféréshez a természetes személy részéről milyen személyes adatok megadása szükséges.

Ugyanakkor a Dáptv.-nek nem tárgya az egyes konkrét elektronikus ügyintézések során történő személyes adatgyűjtések, adatfelhasználások meghatározása, mivel ezek más jogszabályokban, így különösen az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény és más ágazati törvényekben kerültek szabályozásra.

Adattakarékosság: a Dáptv. és végrehajtási rendeletei szerint kezelt személyes adatok az adatkezelési céljai szempontjából megfelelőek és relevánsak, és a szükségesre korlátozódnak. A Dáptv. nem teszi lehetővé olyan személyes adat kezelését, amely az adatkezelés céljához feltétlenül nem szükséges. Ezen túl az adatkezelőknek megfelelő technikai és szervezési intézkedéseket hoznak annak érdekében, hogy az adattakarékosság elve érvényesüljön. A kezelt és tárolt személyes adatok köre a fentiek alapján a szükséges minimum adatok az adatkezelés céljának kielégítésére.

Pontosság: mivel a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük, az adatkezelőknek minden ésszerű intézkedést meg kell tenniük annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék. Ez a Dáptv. előírása hiányában is, a GDPR alapján az érintett adatkezelőket terhelő kötelezettség.

A szervek közötti együttműködésre vonatkozó szabályozás célja elsősorban éppen a pontosság, azaz az állami nyilvántartásokban meglévő adatok pontosságának biztosítása, az ügyintézés megbízhatóságának, az alapul fekvő adatok pontosságának erősítése, az adatbeviteli hibák megelőzése. A digitális állampolgárság ezért a digitális állami nyilvántartásokban kezelt adatokra épül. Az állami nyilvántartások és szakrendszerek egymással összehangoltan működnek.

A szabályozás a vonatkozó adatvédelmi jogi előírások betartásával, az elvek előtérbe helyezése mellett került előkészítésre. Az érintettek számára az adataik kezelésének módja, az esetleges adattovábbítások minden esetben átlátható módon történnek. Az adatkezelés minden esetben a törvényben rögzített céloknak megfelelően és rögzített módon történik, csak az adott cél eléréséhez feltétlenül szükséges mértékben. Az adatkezelés a pontosság érdekében minden lehetséges esetben a közhiteles vagy más, jogszabály alapján hitelesnek tekinthető elsődleges nyilvántartásokban tárolt adatokra épül. A tárolás időtartama előre meghatározott szempontok szerint korlátozott. Az érintettnek minden esetben joga van tájékoztatást kérni az adatkezelő által kezelt adatokról.

Mi az adatmegőrzés időtartama?

Az adatok megőrzésének időtartama alapvetően azon jogszabályokban meghatározott, melyek az adatkezelőket közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához az adatkezelésre kötelezik.

A digitális állampolgárság nyilvántartást vezető szerv a természetes személy adatait a felhasználói profil megszüntetését követő 5 év elteltével zárolja, ezt követően azokat kizárólag a digitális állampolgársághoz kapcsolódó nyilatkozat, valamint az elektronikus azonosítás hitelességének visszavezethetősége, továbbá a polgárok jogai és jogos érdekeinek védelme érdekében a felhasználói profil megszüntetését követő 50 évig kezelheti.

Az érintettek jogainak biztosítására szolgáló intézkedések

Az egyes ügyintézésekhez, digitális szolgáltatásokhoz kapcsolódó adatkezelések vonatkozásában az érintett jogait a hatáskörrel rendelkező szervezet biztosítja, az érintett a hatáskörrel rendelkező szervezet által biztosított módon gyakorolhatja. Az érintett jogainak gyakorlása a Dáptv.-ből fakadó adatkezelések tekintetében az alábbiak szerint biztosított.

Milyen módon tájékoztatják az érintetteket az adatkezelésről?

Az adatkezelésről szóló tájékoztatás a szolgáltatást igénybe vevők számára – az ügyintézési regisztrációt megelőzően, és minden egyes ügyintézéskor – a GDPR 12-14. cikkének (az Infotv. 2. § (3) bekezdése szerinti személyes adatok kezelése esetében az Infotv. 16. §-a alapján) megfelelően a DÁP keretalkalmazásban, illetve az online ügyintéző felületen történik. Ugyanitt elérhető lesz az Általános Szerződési Feltételek (ÁSZF) című dokumentum is.

Amennyiben az adatkezelés hozzájáruláson alapul, milyen módon szerzik be az érintettek hozzájárulását?

Az adatkezelés alapvetően nem az érintett hozzájárulásán alapul, amennyiben igen, annak beszerzése a GDPR 7. cikkével összhangban kell, hogy történjen.

Milyen módon érvényesíthetik az érintettek a hozzáférési, illetve az adathordozhatósághoz való jogukat?

Az érintettek a GDPR 15. cikke szerint érvényesíthetik hozzáférési, és 20. cikkének megfelelően az adathordozhatósághoz való jogukat.

Hogyan gyakorolhatják az érintettek a helyesbítéshez és törléshez való jogukat?

Az érintettek a GDPR 16. cikke szerint gyakorolhatják a helyesbítéshez és a GDPR 17. cikke alapján a törléshez való jogukat, amennyiben az alkalmazandó az adatkezelés jogalapjára tekintettel.

Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához, valamint tiltakozáshoz való jogukat?

Az érintettek a GDPR 18. cikke szerint gyakorolhatják az adatkezelés korlátozásához és 21. cikke alapján a tiltakozáshoz való jogukat.

Az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés?

Az adatfeldolgozóval abban az esetben nem lesz szükség adatfeldolgozási szerződés megkötésére, ha a GDPR 28. cikkében foglaltakat jogszabály vagy más jogi aktus teljeskörűen szabályozza.

Az Európai Unión kívülre történő adattovábbítás esetén megfelelő védelemben részesülnek-e a személyes adatok?

A vizsgált szolgáltatások nyújtása során Európai Unión kívülre történő adattovábbításra várhatóan nem kerül sor.

Tervezett vagy meglévő intézkedések

Fizikai, adminisztratív és logikai védelem

A Dáptv. szerinti szolgáltatások olyan elektronikus információs rendszereken alapulnak, amelyeknek meg kell felelniük az Ibtv. és a végrehajtási rendeletei szerinti követelményeknek. A rendszerek fejlesztésével összefüggésben előzetesen meghatározott IT biztonsági és információvédelmi követelmények is ezen jogszabályokra tekintettel kerülnek meghatározásra.

Mivel gyakorlatilag valamennyi digitális szolgáltatás hátterében működő összes informatikai rendszer helyileg a Kormányzati Adatközpontban kerül elhelyezésre és a meglevő elektronikus információs rendszerek infrastrukturális hátterét jogszabály alapján kötelezően a NISZ Zrt. biztosítja, a fizikai hozzáférés-védelem a lehető legmagasabb szinten lesz biztosított (megfelelve az Ibtv.-nek).

A keretalkalmazást és a háttérrendszereket az Ibtv. és a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény alapján kell megvalósítani, ezért az ezekben foglalt szabályok lesznek irányadók és annak megfelelő tervezési, műszaki intézkedések kerülnek megvalósításra.

A megtett, illetve tervezett konkrét intézkedések:

- Titkosítás
- Logikai hozzáférés szabályozás
- Nyomon követhetőség (naplózás)
- Adatminimalizálás
- Üzembiztonság
- Rosszindulatú software-ek kiszűrése
- Hálózatbiztonság (pl.: tűzfal, tartalomszűrő)
- Szabályzatok
- Az adatokhoz való hozzáférés korlátozása

- Adatfeldolgozóval kötött szerződés rendelkezései
- Adatvédelmi tisztviselő kijelölése
- Fizikai hozzáférés-védelem (pl.: beléptető rendszer, kamerarendszer, behatolás jelző) az adatkezelési műveleteket végző rendszerelemek esetében
- Elkülönítés (fizikai, logikai szeparáció)
- Kiszolgálókon és munkaállomásokon alkalmazott kontrollok (p.: patch management, jelszó-policy, monitoring)
- Mentések
- Hardverek fizikai karbantartása
- Oktatások, tréningek a felhasználók számára.

Általánosan elmondható továbbá, hogy az egyes szervezetek fejlesztései vonatkozásában a védelem magas szintjének biztosítását szolgálja az Állami Alkalmazás-fejlesztési Környezetre vonatkozó szabályozás, azaz az egységes Állami Alkalmazás-fejlesztési Környezetről és az Állami Alkalmazás-katalógusról, valamint az egyes kapcsolódó kormányrendeletek módosításáról szóló 314/2018. (XII. 27.) Korm. rendelet, amely alapján a kijelölt központi alkalmazásszolgáltató és központi termék minőségbiztosító a rendeletben meghatározott módon biztosítja a rendelet hatálya alá tartozó fejlesztések jogszabályoknak megfelelő, és magas színvonalát.

A Kormány rendeletében kijelölt digitális szolgáltatóközpont továbbá az egységesen magas szolgáltatásminőség és védelmi szint érdekében közzéteszi a digitális szolgáltatások és támogató szolgáltatások tervezésére és megvalósítására vonatkozó szabályokat és ajánlásokat, valamint módszertani támogatást nyújt e tevékenységek végzéséhez, az eredményeket folyamatosan figyelemmel kíséri.

Mivel a szabályozott elektronikus ügyintézési szolgáltatások esetében egyes esetekben gazdasági szereplők is megjelenhetnek szolgáltatóként, így e szolgáltatások nyújtásának feltétele a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének rendeletében meghatározott kiberbiztonsági követelményeknek való megfelelés biztosítása és igazolása.

Az adatokhoz való jogosulatlan hozzáférés

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

Az érintettre vonatkozó bármely adat, információ csak akkor ismerhető meg, ha arra az adatigénylőnek megvan a felhatalmazása. Az adatok arra jogosulatlan személyek általi megismerése valószínűsíthetően magas kockázattal járna az érintettekre nézve. Megismerhetővé válnának az állampolgár egyes adatai, dokumentumai, ezáltal személyes adatok sérülnének. Lehetséges társadalmi-politikai hatásként bizalomvesztés merülne fel a technológiával és az érintett intézményekkel szemben. A legfőbb kockázat az adatok nyilvánosságra kerülése.

Mely fő fenyegető veszélyek idézhetik elő a kockázatot?

A jogosulatlan hozzáférés kockázata alapvetően az érintett oldalán merülhet fel. Például elveszíti mobil eszközét, arra jogosulatlan személy számára hozzáférhetővé teszi személyes adatait. Másfelől bűncselekmény útján kerülhet sor a hozzáférésre.

A kockázat forrása lehet emberi hanyagság, vagy olyan infrastruktúra hiba, melynek következtében illetéktelen személyek jogosulatlanul hozzáférnek a szerveren tárolt személyes adatokhoz, így:

- alkalmazás gyenge pontjai,
- nem megfelelően kontrollált hozzáférés,
- hálózati gyenge pontok (pl. tűzfal engedélyezési problémák),
- titkosítás nem megfelelő,
- külső vagy belső visszaélés,
- rendszer ellen történő támadás,
- rendszer hiányosságának / gyengeségének kihasználása,
- kompetencia hiánya, emberi hanyagság.

Melyek a kockázat forrásai?

Informatikai rendszer meghibásodás, vagy – az esetek döntő részében – emberi tényezőkből fakadó kockázatok, melyeket figyelemfelhívással, tájékoztatással lehet mérsékelni, de kizárni nem lehet. Ilyenek lehetnek:

- Jelszólopás/átadás.
- Rendszerbelépési jogosultsággal rendelkező közreműködő adatlopása.
- Szerverterem/szerver oldali hálózat forgalmának figyelése, elemzése, titkosító kulcs feltörése, megismerése.
- Kártékony kód számítógépen való futtatása, melynek következtében illetéktelen személyek jogosulatlanul hozzáférhetnek a meghajtón lévő személyes adatokhoz.
- Adatszivárgás útján (pl. egy fizikai adathordozóra kerülnek az adatok, amit jogosultsággal nem rendelkező személyek is látnak.).
- Informatikai rendszer meghibásodása.

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Auditált IT rendszerek útján biztosított információvédelem, fizikai hozzáférés-védelem, adminisztratív, szervezeti védelem (szabályzatok, adatfeldolgozói szerződések rendelkezései, stb.). Továbbá figyelemfelhívás, tájékoztatás a felhasználók számára, oktatások. Az adatok titkosított tárolása, a hozzáférések naplózása. Rosszindulatú szoftverek szűrése.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A kockázat súlyossága jelentős.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A kockázat valószínűsége korlátozottan becsülhető, mivel azok döntő részben emberi tényező függvényei (gondatlanságon vagy bűncselekményen alapul a kockázat bekövetkezése).

Az adatok véletlen vagy jogellenes megváltoztatása

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

Az adatok véletlen vagy jogellenes megváltoztatása valószínűsíthetően magas kockázattal járna az érintettre nézve. Az adatok jogellenes megváltoztatása esetén személyes adatok sérülnének, amely az állampolgár ügyintézésére kihatással lehet. Lehetséges társadalmi-politikai hatásként

bizalomvesztés merülne fel a technológiával és az érintett intézményekkel szemben.

Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?

Amennyiben nem biztonságos informatikai környezetben működtetett IT rendszerben, hanem pl. egyszerű irodai alkalmazásokban (pl. MS Excel) történne az adatkezelés, de a fentebb jelzett IT biztonsági és üzemeltetési előírások miatt ilyen nem történhet meg. Veszélyt jelenthet továbbá az infrastruktúra esetleges sérülékenysége, így:

- hálózati gyenge pontok (pl.: nem áll rendelkezésre az adott telekommunikációs szolgáltató által biztosított megfelelő sávszélesség, tűzfal engedélyezési problémák),
- titkosítás nem megfelelő volta,
- külső vagy belső visszaélés,
- rendszer ellen történő támadás,
- rendszer hiányosságának / gyengeségének kihasználása,
- kompetencia hiánya, hanyagság.

Ezen felül a jogellenes hozzáférésnél leírtak is veszélyt jelenthetnek.

Melyek a kockázat forrásai?

A gyenge IT infrastruktúra és IT biztonsági környezet az adatgazda közfeladatot ellátó szervek oldalán. Ezen felül a jogellenes hozzáférésnél leírtak is kockázatot jelenthetnek.

A megadott intézkedések közül melyek megfelelőek a kockázatok kezelésére?

Fizikai és logikai hozzáférés-védelem, auditált IT rendszerek útján biztosított információvédelem, mentési rendszerek, amelyekből az adatok szükség esetén visszaállíthatók. Ezen felül a jogellenes hozzáférésnél leírtak itt is irányadóak.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A kockázat súlyossága jelentős.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A kockázat valószínűsége korlátozottan becsülhető, mivel azok döntő részben emberi tényező függvényei (gondatlanságon vagy bűncselekményen alapul a kockázat bekövetkezése).

Adatvesztés

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

Az adatvesztés valószínűsíthetően magas kockázattal járna az érintettre nézve. Az adatvesztés esetén személyes adatok sérülnének, amely az állampolgár ügyintézésére kihatással lehet. Lehetséges társadalmi-politikai hatásként bizalomvesztés merülne fel a technológiával és az érintett intézményekkel szemben.

Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?

Nem várt informatikai rendszer leállások, incidensek, katasztrófák (vis maior). Veszély az infrastruktúra esetleges sérülékenysége, így:

- hálózati gyenge pontok (pl.: nem áll rendelkezésre az adott telekommunikációs szolgáltató által biztosított megfelelő sávszélesség, tűzfal engedélyezési problémák),
- titkosítás nem megfelelő,
- külső vagy belső visszaélés,
- rendszer ellen történő támadás,
- rendszer hiányosságának / gyengeségének kihasználása,
- kompetencia hiánya, hanyagság.

Ezen felül a jogellenes hozzáférésnél leírt fenyegetések is fennállnak.

Melyek a kockázat forrásai?

Állami informatikai rendszerek esetleges sérülékenysége. Ezen felül a jogellenes hozzáférésnél leírt kockázatforrások is felmerülhetnek.

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Auditált IT rendszerek útján biztosított információvédelem, Fizikai hozzáférés-védelem, mentési

rendszerek, amelyekből az adatok szükség esetén visszaállíthatók. Ezen felül a jogellenes hozzáférésnél leírt intézkedések is védelmet biztosítanak az adatvesztés megelőzésére.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A redundáns állami informatikai rendszerekben az adatvesztés kockázatának súlyossága elhanyagolható mértékű, mert mentett állományokból az elveszett adatok visszaállíthatóak.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

A redundáns állami informatikai rendszerekben az adatvesztés kockázatának súlyossága elhanyagolható mértékű, mert mentett állományokból az elveszett adatok visszaállíthatóak.

A hatásvizsgálat eredménye

A kockázatértékelés alapján a vizsgált adatkezelés – az adatkezelő által az adatkezeléssel járó kockázatok mérsékléséhez szükséges intézkedések figyelembevételével – valószínűsíthetően nem jár magas kockázattal az érintettekre nézve. Így a tervezett adatkezelés vonatkozásában nem állnak fenn az Infotv. 25/H. §-ában foglaltak. A tervezett szabályozással kapcsolatos adatvédelmi szempontú felülvizsgálat a jogszabály-tervezet közigazgatási egyeztetése keretében valósul meg.

Tekintettel arra, hogy a Dáptv. a digitális szolgáltatás nyújtásához szükséges adatkezeléseket részletesen nem szabályozza, és az a Kormánynak ad felhatalmazást arra, hogy azokat a későbbiekben rendeletben szabályozza, továbbá a műszaki megvalósítás számos aspektusa a jogalkotás jelen szakaszában még számos adatkezelés tekintetében nem ismert, így az adatkezelésből eredő konkrét kockázatok teljes körűen nem azonosíthatóak be.

A fentiekre figyelemmel a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatásának megfelelően [lásd: Jogszabálytervezetek adatvédelmi hatásvizsgálata - Nemzeti Adatvédelmi és Információszabadság Hatóság (naih.hu)] – a jelen hatásvizsgálat az adatkezelés részletes szabályaira tekintettel a jövőben (a rendszer éles indulását megelőzően) kiegészítésre kerül, különösen a kockázatok feltérképezésének részletezése körében, továbbá szükség szerint intézkedési terv elkészítésére kerül sor. Ezen kiegészítést követően tehető pontosabb állásfoglalás abban a kérdésben, hogy a tervezett adatkezelés vonatkozásában fennállnak-e az Infotv. 25/H. §-ában foglaltak.