HADMÉRNÖK

XIV. Évfolyam 2. szám – 2019. június

10.32567/hm.2019.2.23

A FENNTARTHATÓ ÉS ZAVARTALAN ELEKTRONIKUS ÜGYINTÉZÉS SZOFTVERTECHNOLÓGIAI HÁTTERE - 1. RÉSZ

THE TECHNICAL BACKGROUND OF SUSTAINABLE AND CONTINUOUS ELECTRONIC ADMINISTRATION - 1. PART

GEREVICH János; NÉGYESI Imre

(ORCID: 0000-0001-7236-4514); (ORCID: 0000-0003-1144-1912)

gerevich.janos@agilexpert.hu; negyesi.imre@uni-nke.hu

Absztrakt

Európán innen és túl az egyes országok mindenkori törvényhozásának mindig is nehézséget jelentett az új technológiákkal együtt kialakult kérdések időben történő szabályozása. Az új kihívások feltárása és megértése során a nemzetközi gyakorlat nyomon követése adhat támpontokat, természetesen az adott ország sajátosságainak figyelembe vételével. Napjaink információs társadalmában folyamatosan szabályozandó terület az e-kormányzás is. A leendő korok generációinak már magától értetődő lesz a digitális alapokon megvalósuló kormányzás, ugyanakkor a szabályozás és a megvalósítás manapság még érdekes kérdéseket vet fel. Ebben a tanulmányban a GDPR és az elektronikus ügyintézéssel kapcsolatos követelmények szoftvertechnológia elemzése következik. A cikk második felében a szerzők a feltárt problémák kezelésére alkalmas szoftvertervezési mintákat mutatnak be.

Kulcsszavak: *Általános Adatvédelmi Rendelet, elektronikus ügyintézés, szoftvertechnológia, tervezési minta, proxy, holder*

Abstract

In Europe and anywhere in our well-known world, the timely handling of problems caused by new technologies has always been difficult for the legislation. During the exploration and understanding of the new challenges, the international practice can provide a point of reference according to the specialties of the country. In today's information society, e-Government is an area to be constantly regulated. For the next generations, the digital government will be self-evident, but the regulation and the implementation face with interesting issues today. In this paper, the GDPR and the electronic administration related requirements will be analyzed from the software technology perspective. In the second part of the article authors present software design patterns that can be used to solve the identified problems.

Keywords: *GDPR, electronic administration, software technology, design pattern, proxy, holder*

A kézirat benyújtásának dátuma (Date of the submission): 2019.04.11.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.04.26.

BEVEZETÉS

A létfontosságú infokommunikációs rendszerek védelmére vonatkozó Uniós és hazai szabályozás egy átfogó keretet határoz meg a kibertérben fellelhető különböző fenyegetések kapcsán. Magyarországon az információbiztonság kérdéskörével a 2011. évi CXII. törvény foglalkozik az információs önrendelkezési joggal és az információszabadsággal [1] (röviden: Infotv.). Jelenlegi állapotát 2018.07.26-ai módosítását követően nyerte el összhangban az Európai Parlament és Tanács (EU) 2016/679 rendeletével, a GDPR-al [2], amely a személyes adatok védelméről rendelkezik az Európai Unión belül. A szabályozás célja egy országhatárokon átívelő, átlátható és nyomon követhető adatkezelési- és adatfeldolgozási rendszer kialakítása.

Hazai viszonylatban 2018. január 1-én lépett életbe az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény [3], amely lefekteti az elektronikus ügyintézés alapjait és meghatározza azokat a szolgáltatásokat és kötelezettségeket, amelyek a korszerűbb közszolgáltatások nyújtásához szükségesek. Mindkét dokumentumban gyakran jelennek meg az adatok megőrzésével, törlésével kapcsolatos elvárások. Jelen tanulmány feltárja az iménti jogszabályokból levezethető informatikai követelményeket, majd az azonosított követelményrendszerre szoftvertervezési mintákon keresztül ad megoldást.

A GDPR áttekintése

A magyar köztudatban is GDPR-ként (angolul: General Data Protection Regulation) jelent meg az Európai Unió Általános Adatvédelmi Rendelete. A dokumentum 2018. május 25-én lépett hatályba, ezzel sok fejfását okozva azoknak az állami és nem állami szervezeteknek, amelyek a hatálya alá tartoznak. Azonnal felmerülhet a kérdés a szakterületet kevésbé ismerőknek, hogy valóban szükség volt-e egy ekkora horderejű rendeletre? Cinikusabban is fel lehet tenni a kérdést: a brüsszeli bürokrácia újra alkotott valamit? A szabályozás létjogosultságát azonban nehéz lenne tagadni, mert ugyan tagállami és Uniós szinten is léteztek már a területet szabályozó dokumentumok, de az EU kiberbiztonságának javításához egy új, átfogó rendeletre volt szükség.

Miért leszek attól nagyobb „kiberbiztonságban”, ha minden velem kapcsolatban álló jogi személy számára hozzájáruló nyilatkozatot kell kitöltenem a személyes adataim kezelésével kapcsolatban? Erre a kérdésre a válasz maga a GDPR. A rendelet részletes feltárása előtt érdemes szót ejteni a napjainkban egyre nagyobb teret nyerő kiberbűnözésről. Megjelentek a zsaroló és adatlopó vírusok, melyek alapvetően otthoni notebookokról lophatnak adatokat, ugyanakkor egy feltört vírusos számítógép lehetővé teheti egy teljes informatikai rendszer feltörését is. Célzott támadások mögött lehetnek hacker csoportok, titkosszolgálatok, de az ipari kémkedés is előfordulhat, mint kiváltó tényező. Ha emellett azt is szem előtt tartjuk, hogy az Európai Unió belső piacán működő infokommunikációs rendszerek országhatárokon átnyúló fénysebességű sztrádán terjesztik személyes adatainkat egy-egy online vásárlás, regisztráció, valamilyen szolgáltatás igénybe vétele során, azonnal érthetővé válik, hogy a kiberbiztonsági kockázat jelentékeny biztonsági tényezővé vált napjainkra. [4] Az Általános Adatvédelmi Rendelet célkitűzése, hogy személyes adataink szabályozott módon kerüljenek be a velünk kapcsolatban álló szervezetek informatikai nyilvántartásaiba, adataink továbbadása, feldolgozása követhető módon történjen. A rendeletben külön hangsúlyt kap a személyes adatok törlésének kérdése, csökkentve a biztonsági kockázatot – ha nincs adat, akkor nincs mit ellopni.

Az általános rendelkezésekből [2; 1. fejezet] megtudhatjuk, hogy a rendelet célja alapvetően a természetes személyek adatainak védelme és a személyes adatok szabad áramlásának

szabályozása az EU területén belül[1]. Az általános szabályozás alól kivételt képezhetnek az egyes tagállamok védelmi szektoraiban tevékenykedő különböző szervezetek. A precíz megértéshez szükséges a GDPR fogalom-meghatározásaiból [2; 1.4] néhányat felsorolni az alábbiakban.

1. *„„személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ;*
2. *„adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;*

   …
3. *„adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza;*
4. *„adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;”*

A személyes adat definíciójában találkozhatunk az érintett fogalmával, aki az a természetes személy, akinek a személyes adatait az adott nyilvántartás tárolja. Az érintett azonosított, ha direkt módon kinyerhető a tárolt adatokból az érintett kiléte. Azonosítható az érintett, ha egy vagy több adat alapján közvetlen vagy közvetett módon feltárható a természetes személy kiléte.

Az adatkezelés végzése során – amely a személyes adatokon végzett „tetszőleges” műveletet takar – az adatkezelőknek igazolniuk kell a tevékenység jogszerűségét, amelyre felhatalmazást adhat az érintett saját maga vagy valamilyen szerződés, illetve egy tagállami vagy uniós jogszabály is megkívánhatja valamilyen adatkezelési tevékenység végzését. A felsoroltakon túl további kivételes helyzetekben is jogszerű lehet a személyes adatokon végzett adatkezelés, ezeknek a jogosítványoknak harmóniában kell lenniük az uniós joggal – részletesen a második fejezet, hatodik cikk foglalkozik a témakörrel. [2; 2.6.(2)-(4)] Az adatfeldolgozók a GDPR vonatkozásában az adatkezelőktől örökölik meg a felhatalmazást a személyes adatokon végzett tevékenységükre. Mind az adatkezelőknek és az adatfeldolgozóknak is tevékenységüket jogszerű, tisztességes és átlátható eljárás keretein belül kell végezniük. Továbbá, a *célhoz kötöttség*, az *adattakarékosság*, a *pontosság*, a *korlátozott tárolhatóság*, az *integritás* és a *bizalmas jelleg* sorolhatók azon alapelvek közé, amelyekért az adatkezelő felelősséggel tartozik. [2; 2.5.(1)-(2)].

Attól függetlenül, hogy egy jogszabály, szerződés vagy az érintett hozzájárulása teremt jogalapot az adatkezelésre az érintett mindenkori hozzáférési joggal rendelkezik ahhoz, hogy információt kapjon a személyes adataival kapcsolatos adatkezelési folyamatokról, az adatkezelés céljáról és az kezelt személyes adatok kategóriáiról. [2; 2.15] Ha bekövetkezik ez az esemény, akkor a kézi fizikai- vagy digitális nyilvántartást vezető adatkezelőknek is gondot okozhat a fenti információk egy időben történő, pontos összegyűjtése és az adatszolgáltatás. Ennél sokkal összetettebb problémát jelenthet az automatizált módon történő adatkezeléssel kapcsolatos információk kinyerése.

A továbbiakban a digitális alapokon működő automatizált adatkezelés és adatfeldolgozás kérdéskörét vizsgáljuk. A vizsgálat során megpróbáljuk tetten érni az informatikában jól ismert

[1] A GDPR 1. fejezet 3. cikk foglalkozik a területi hatállyal

CRUD műveleteket[2], melyek az adatok olvasását, létrehozását, módosítását, valamint törlését fogják össze. Az iménti példában egy létrehozási (CREATE) és olvasási (READ) műveletre vonatkozó követelményre derült fény – az adatkezelési tevékenység feltételezi a személyes adatok mentését, míg a hozzáférési jog azok olvasását. Az Általános Adatvédelmi Rendelet konkrét követelményeket fogalmaz meg a személyes adatok helyesbítését és törlését illetően is [2; 2.16-17], ezáltal a személyes adatokra vonatkozó módosítás (UPDATE) és törlés (DELETE) műveletek is megjelennek a követelményrendszerben. A GDPR és az Infotv. által meghatározott CRUD műveletek problémakörének tárgyalásához nem szükséges az említett dokumentumok további elemzése, mindkét dokumentum olyan speciális jogi eseteket tárgyal, ahol valamelyik CRUD művelet végrehajtása részben, illetve egyáltalán nem végezhető el. Például közhatalmi szervek által lefolytatott eljárások, ügyészségi-, bírósági feladatok, stb. A kivételt képező esetek tárgyalása túlmutat az alapvető szoftvertechnológiai problémán, miszerint: Milyen adatmodell képes helyesen és jogszerűen kezelni a működés során felmerülő olvasási, létrehozási, módosítási és törlési műveleteket az érintettek személyes adatainak vonatkozásában? Az 1. ábrán az érintettek személyes adatai és az adatkezelési tevékenységek során keletkező egyéb információk kapcsolatát láthatjuk.

1. ábra Az érintett személy adatai és az adatkezelés során keletkező információk közötti kapcsolat primitív modellje. SOK-SOK kapcsolat (saját szerkesztés)

A bemutatott modell feltételezi, hogy egy érintettnek akár több jogalappal is lehetnek különböző adatai egyazon informatika rendszerben, nyilvántartásban. Bizonyos tekintetben az is elképzelhető, hogy az adatkezelési tevékenységek során több *Érintett* adatai is kapcsolódhatnak egyazon adatkezelési információhoz. Példa lehet erre egy online rendelés, ahol címzett és a vevő két különböző természetes személy. Vizsgáljuk meg ezt a modellt a CRUD műveletek szemszögéből.

1. CREATE – a létrehozás során az érintett minden személyes adata egy helyen kerül tárolásra, ha egy rendszerben több adatkezelési tevékenységet is folytatnak, akkor sérülhet az adattakarékosság elve, mert több adat is bekerülhet a rendszerbe, mint ami feltétlenül szükséges.
2. READ – adatszolgáltatási kötelezettségből vagy az adatkezelési tevékenységből fakadó folyamatok számára szükséges olvasási művelet. Ebben a modellben az érintettnek mindig egy aktív személyes adata van a nyilvántartásban. Ha több adatkezelési eljárás is történt az érintett személyét vonatkozóan, nehézkes egy korábbi cím, tetszőleges adat kinyerése a rendszerből. Eseménynaplók segítségével kezelhető a probléma, de az adatok kinyerése nehézkessé válhat.
3. UPDATE – helyesbítési igény vagy egy adatkezelési tevékenység során végrehajtandó módosítás abban az esetben, ha a nyilvántartásban több aktív adatkezelési tevékenység is zajlik egyazon érintett vonatkozásában inkonzisztens állapotot válthat ki. Teljes

[2] CRUD műveletek – mozaikszó a **C**REATE **R**EAD **U**PDATE **D**ELETE angol szavak kezdőbetűiből, magyarul: létrehozás, olvasás, módosítás, törlés

egészében vagy részben sérülhetnek az érintett személyes adatai valamelyik folyamatban lévő adatkezelési tevékenységben, ezáltal hibás folyamatok indulhatnak.

4. DELETE – a törlés művelete a GDPR vonatkozásában került igazán előtérbe, addig nem szívesen foglalkoztak a szoftvermérnökök az adatokon végzendő törlés művelet problémájával. Azok a rendszerek, amelyek az Általános Adatvédelmi Rendelet hatálya alá tartoznak már kötelesek a korlátozott tárolhatóság elvét figyelembe venni, így bizonyos időközönként, illetve az érintett kérésére fizikailag törölniük[3] kell az érintett személyes adatait egy-egy adatkezelési tevékenység vonatkozásában. Egy ilyen művelet sértheti az informatikai rendszer integritását, például abban az esetben, ha több párhuzamos adatkezelési tevékenység végrehajtása zajlik egy időben.

A fizikai- és a logikai törlés összehasonlítása

Évtizedeken át a szükségtelenné vált adatok logikai törlése[4] volt a bevett gyakorlat az informatikai rendszerek tervezése során. Ennek oka főleg az volt, hogy egy programhiba esetén az adatok visszaállítása, visszaépítése sokkal egyszerűbb feladat volt, mint egy fizikai törlés esetén. Ugyanakkor itt azt is meg kell jegyezni, hogy ez a technika vezetett ahhoz is, hogy az ily módon tervezett rendszerekben az adattisztítás szinte lehetetlenné vált az évek múlásával – ezáltal biztonsági kockázatot teremtve a külső és belső kockázatok területén is.

1. Fölöslegesen tárolt adatok – adatlopás;
2. Törölt, inaktív adatok – nehézkes továbbfejlesztés, körülményes adattisztítás;

A problémát tovább tetézi az a tény is, hogy komolyabb jogfolytonosság tanúsítására képes rendszerek esetében egy tetszőleges entitás adatai többször változhatnak az évek során és csak évek múltával kerülhet törlésre az entitáshoz tartozó összes adat.

Az 1. ábrán bemutatott primitív modell önmagában kevésnek bizonyul a fizikai törlés támogatására. Lehetséges választás lehet a 2. ábrán szereplő *Proxy* tervezési minta alkalmazása, ahol a kliens objektumhoz tartozhat több proxy objektum, melyeken keresztül a kliens üzenetet válthat az ún. proxizott objektumokkal. Az ábrából kiderül, hogy a *Proxy* mindig a proxizott objektum felé továbbítja az üzeneteket. Valamint egy proxizott objektumhoz egy időben tartozhat több *Proxy* is. Vizsgáljuk meg ezt az alapvető tervezési mintát a proxizott objektum fizikai törlésének szempontjából. Amennyiben bekövetkezik a DELETE művelet a *Proxy* nem tudja tovább továbbítani kliens üzeneteit a proxizott objektum felé, mert az már nem létezik – így jó esetben hibaüzenetet, rossz esetben hibát produkál a modell.

2. ábra Proxy tervezési minta (saját szerkesztés)

Létezik a *Proxy* tervezési mintához nagyon hasonló, ugyanakkor más elven működő tervezési minta a *Holder* (magyarul: tartó). A *Holder* felépítését és működési elvét a 3. ábra mutatja be, miszerint különböző kliensekhez, különböző *Holder*-ek tartozhatnak. A *Holder* ismeri a megtartott objektumot és a kliens kérésére átadja azt a kliens számára. A modell lényege, hogy nem kell a klienshez folyamatosan betölteni az összes megtartott objektumot, elegendő megtenni azt akkor, amikor a kliens konkrét üzenetküldést kezdeményezne. Utóbbi

[3] Fizikai törlés – egy adatrekord végleges, visszavonhatatlan eltávolítása az adatbázisból
[4] Logikai törlés – egy adatrekord törölt állapotának jelzése egy igaz/hamis kapcsoló segítségével.

viselkedés a *Proxy* esetében is hasonló. A megtartott objektum fizikai törlésekor a *Holder* egy NULL objektumot ad vissza, melyet a kliens már kezelhet, természetesen, ha fel van rá készítve.

3. ábra Holder tervezési minta (saját szerkesztés)

A bemutatott *Proxy* és *Holder* tervezési minták önmagukban nem képesek kezelni a fizikai törlés problémáját. További finomításra van szükséges a zavartalan adatkezelési tevékenység támogatásához.

Az ÉrintettHolder tervezési minta

Fontos tisztázni, hogy az érintett személyes adatait a megtartott objektum, illetve a proxizott objektum jelentik a fenti modellekben. A *Proxy* tervezési minta legnagyobb problémája a folyamatban lévő adatkezelési tevékenység szempontjából, hogy a modell állapotmentes, tehát csak továbbítja az üzeneteket. Ha a proxizott objektum törlődik, akkor az esetek jelentős részében az adatkezelési folyamat sérülhet adatvesztés következtében. A *Holder* tervezési minta esetében minimális állapot már megjelenik, ha a kliens elkéri a *Holder*-től a megtartott objektumot, akkor annak létezése eldönthető. A GDPR-ban megjelenő követelmények az érintett irányából vizsgálják a problémát, így kézenfekvő a modell irányának megfordítása és a probléma vizsgálata az *Érintett* irányából, valamint a *Holder* tervezési minta ötvözése a *Proxy* tervezési mintával az alábbiak szerint. Az így kialakult tervezési mintát a 4. ábra mutatja be.

4. ábra ÉrintettHolder tervezési minta (saját szerkesztés)

1. CREATE – minden adatkezelési folyamat minden használati esetében az *Érintett* és az *Adatkezelési tevékenységhez köthető információ* között létre kell hozni egy *ÉrintettHolder* típusú objektumot, amely a következő tulajdonságokkal rendelkezik.
2. READ – amíg aktív az adott adatkezelési tevékenység, addig proxyként továbbítja az üzeneteket az *Érintett* irányába.
3. UPDATE – amennyiben a teljes adatkezelési folyamat vagy egy mozzanata véget ér akkor az *ÉrintettHolderben* tárolásra kerülnek a konkrét adatkezelési tevékenységhez kapcsolható személyes adatok, amennyiben megváltoznak az Érintett személyes adatai, az ÉrintettHolder az egykor aktív történetileg helyes adatokat fogja tartalmazni.
4. DELETE – ha valamilyen okból törölni kell az *Érintettet* a teljes informatikai nyilvántartásból vagy bizonyos adatkezelési tevékenységekhez kapcsolódóan, akkor az *Érintett* fizikai törlése megoldott, ugyanis az *ÉrintettHolder* tovább tárolhatja egy adott folyamat számára releváns adatokat, ha van valamilyen követelmény erre vonatkozóan. Ha valamilyen okból kifolyólag minden információt törölni kell az *Érintettről* bele értve minden *ÉrintettHolder*-t is, akkor egy ÜRES *Érintett* elem bevezetésével és a kapcsolódó *ÉrintettHolder*-ek ürítésével és az ÜRES elemre történő átirányítással ez a folyamat is kezelhető. Természetesen ez a folyamat csak megfelelő körülmények mellett indítható el – az informatikai rendszert fel kell készíteni az ÜRES elem létezésére, illetve az *Érintetthez* kapcsolódó folyamatban lévő adatkezelési folyamatok megszűnését eredményezi nagy valószínűséggel egy ilyen művelet.

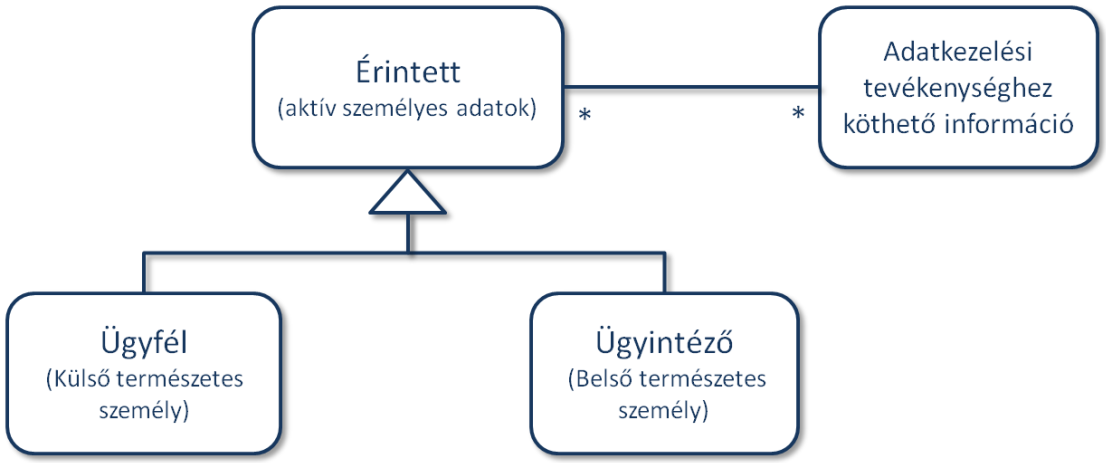
A bemutatott *ÉrintettHolder* tervezési minta a természetes személyek adataihoz kapcsolódó CRUD műveletek kezelésére egy átfogó megoldást kínál, de nem ad választ az elektronikus ügyintézéssel kapcsolatos követelményekre. A 2015. évi CCXXII. törvény által felölelt két fő terület közül az elektronikus ügyintézés probléma köre az, amely a GDPR kapcsán tárgyalt problémákkal is találkozik, még akkor is, ha a GDPR korlátozási lehetőséget biztosít a tagállamok számára, hogy bizonyos területeken [2; 3.23] az érintettek személyes adatait véglegesen, illetve hosszabb távon, nagyobb adattartalommal tárolják. A kivételt képező jogszabályokban törekedni kell arra, hogy a természetes személyek alapvető jogai ne sérüljenek, és a szabályozás megfeleljen a demokratikus normáknak.

Fontos kiemelni, hogy attól függetlenül, hogy a felhatalmazás adott a kivételek képzésére jogszabályi szinten, a személyes adatokhoz tartozó karbantartási műveletek problémája ezekben a rendszerekben is jelen van, legfeljebb más hatások váltják ki azokat. Egyszerű példával élve: egy online vásárlás ügymenete nagyban hasonlítható egy hatósági igazolás igénylési folyamatához – kérelemre-igazolás; megrendelésre-áruszállítás – egy menet közben megváltozott postázási cím kezelése mindkét esetben elvárható követelmény lehet. A webshop esetében a vásárló kérheti a személyes adatainak azonnali törlését a szállítást követően, míg egy állami szerv felmentéssel rendelkezhet az adatok törlése alól. Érdekes kérdés azonban, hogy meddig őrizheti meg az adott állami szerv az ügyfél adatait. A személyes adatok vonatkozásában értelmezhető egyfajta elévülés, előbb-utóbb a törlés művelet igénye is megjelenhet az informatikai rendszerben. Itt kérdés lehet az, hogy az adott rendszer mennyire van felkészítve az ilyen jellegű műveletekre. Az alábbiakban az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvény [3] elemzése következik a természetes személyek adatain végzett CRUD műveletek szemszögéből.

1. CREATE – az elektronikus ügyintézést biztosító szerv és az ügyfél elektronikus kapcsolatára vonatkozó szabályozás értelmében *„Magyarországon az ügyfelet megilleti a jog, hogy az elektronikus ügyintézést biztosító szerv előtti ügyét – az e törvényben meghatározott módon – elektronikusan intézze”.* [3; 1.3.(1)]
2. READ – a közérdekből nyilvános adatok megismerhetőségének biztosítása, és a személyes adatok védelme megjelenik követelményként a 3. fejezetben [3; 1.7].
3. UPDATE – még ebben a fejezetben találkozhatunk a következő követelménnyel, mely szerint *„az elektronikus ügyintézést biztosító szerv az elektronikus ügyintézést támogató és a jogszabályban előírt feltételeket biztosító rendszerfolyamatokat az ügyfél érdekeinek figyelembevételével alakítja ki.”* [3; 1.6.(2)]. Az ügyfél kényelmét szolgáló funkciókon túl, az *„ügyfél igényelheti, hogy az általa meghatározott adatainak változásáról a”…„meghatározott elektronikus ügyintézést biztosító szervet”* [3; 4.22.(2).a] automatikusan vagy esetileg elektronikus úton értesítse az illetékes szolgáltató.
4. DELETE – a szabályozott elektronikus ügyintézési szolgáltatások kapcsán megjelenik a törlés műveletre vonatkozó követelmény. Az ügyfél-regisztrációs nyilvántartást kezelő szervnek meg kell tudnia szüntetni egy regisztrációt, például abban az esetben, ha a felhasználó kéri azt vagy más hivatalos értesülés alapján. [3; 4.32.(5)] Ez jelenthet fizikai, illetve logikai törlést is az elektronikus ügyintézést biztosító szervek informatikai rendszerében, amikor értesülnek a regisztráció megszűnéséről.

Az összegyűjtött követelmények hatásainak az elektronikus ügyintézését biztosító szervek informatikai rendszereiben is meg kell jelenniük. Ha az elektronikus ügyintézés folyamatát vizsgáljuk, akkor az érintett személy az esetek túlnyomó részében ügyfélként jelenik meg, ugyanakkor nem lehet elmenni amellett sem, hogy az ügy intézéséért felelős személy is lehet érintett, amikor a személyes adatai megjelennek az ügyintézési folyamatban. Utóbbi esetben is

megjelennek a CRUD műveletek, amikor a természetes személy felvételre kerül az elektronikus ügyintézést biztosító szerv (CREATE) informatikai rendszerében. Olvasási művelet (READ) kerül végrehajtásra, amikor az ügyintéző személyes adatai megjelennek az ügyintézés egyes mozzanataihoz köthetően. Ezzel párhuzamosan az ügyintéző személyes adatai módosulhatnak (UPDATE) – akár a név is, például házasságkötés miatt. Illetve az ügyintéző munkaviszonya megszűnhet, ekkor bekövetkezhet a törlés művelete (DELETE) is. Az ügyintézésre úgy is tekintünk, mint egy speciális adatkezelési tevékenységre, ebben az esetben az ügyfél és az ügyintéző is lehet érintett a személyes adatok változásának tekintetében, ezt a gondolatmenetet mutatja be az 5. ábra.



5. ábra Az érintett fogalmának kiterjesztése (saját szerkesztés)

Az 1. ábra tárgyalását követően már láthattuk, hogy a CRUD műveletek egy ilyen primitív modellben problémákba ütközhetnek. A továbbiakban az ÉrintettHolder tervezési minta kiterjesztését mutatjuk be a külső kapcsolattartás és folyamatos ügymenet támogatása érdekében.

Zavartalan külső kapcsolattartás

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényből kinyert követelmények alapján látható, hogy az elektronikus ügyintézést biztosító szerv informatikai rendszerének képesnek kell lennie kezelni az ügyfél személyes adataival kapcsolatos CRUD műveleteket. Az 6. ábrán szereplő *ÜgyfélHolder* tervezési minta felépítését tekintve analóg a már korábbiakban bemutatott *ÉrintettHolder*-rel.

6. ábra ÜgyfélHolder tervezési minta (saját szerkesztés)

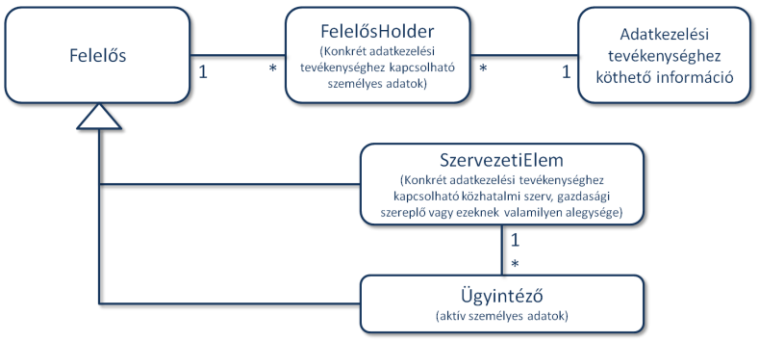
Az alábbiakban az *ÜgyfélHolder*-en értelmezett elektronikus ügyintézés kapcsán felmerülő CRUD műveletek működése kerül bemutatásra. Az *ÜgyfélHolder* működése az általános adatkezelési folyamatokat kezelő *ÉrintettHolder* tervezési minta viselkedésének ügyintézési folyamatokra történő leképezéséből vezethető le.

1. CREATE – minden *Ügyfél* által indított ügyintézési folyamat során létre kell hozni egy *ÜgyfélHolder*-t is az elektronikus ügyintézést biztosító szerv informatikai rendszerében a párhuzamosan folyó ügyintézési folyamatok végett.
2. READ – Egy folyamatban lévő, illetve lezárt ügy vonatkozásában az *Ügyfél* aktív adatainak kinyerése történhet az *Ügyfélből*, illetve egy lezárt ügy esetén az *ÜgyfélHolder*-ből.
3. UPDATE – Az egyes ügyintézési folyamatok sajátossága lehet, hogy az *Ügyfél* aktív adatainak módosítása már nincs hatással minden *ÜgyfélHolder*-re. Az érintett természetes személy – jelen esetben ügyfél – levelezési címének változáskor az ügyfél eredeti postai címét reprezentáló *ÜgyfélHolder*-t már nem feltétlenül kell megváltoztatni.
4. DELETE – Az *ÉrintettHolder* tervezési mintával analóg módon a teljes fizikai törlés is támogatható, de ügytípusonként is eljárhat az elektronikus ügyintézést biztosító szerv.

Az *ÜgyfélHolder* tervezési minta alkalmazása lehetővé teszi a zavartalan külső kapcsolattartást és az ügyfelek személyes adatainak magas szintű kezelését a GDPR alapelveivel összhangban.

Folyamatos ügyintézés fenntartása

Egy elektronikusan keletkezett és intézett ügy életútját összetett folyamatok adják. Az elektronikus ügyintézést biztosító szervnek képesnek kell lennie befogadni az ügyindító dokumentumot, ezt követően szabályozott módon kell párbeszédet folytatni az ügyféllel. Az ügyféllel történő kapcsolattartáson túl nagyon lényegesek ügyintézést támogató belső folyamatok is.



7. ábra FelelősHolder tervezési minta (saját szerkesztés)

Az ügyintézési tevékenység azon túl, hogy legalább egy ügyintézőhöz – természetes személyhez – köthető még általában kapcsolódik egy szervezeti elemhez is. A kapcsolódó szervezeti elem feladatai közé tartoznak a helyettesítés és az ügyintéző változás problémáinak kezelése. Ebből következik az a felismerés, hogy az ügyintézési tevékenység *SzervezetiElem*-hez és *Ügyintéző*-höz is egyaránt köthető és kötendő. A 7. ábrán az is látható, hogy a *SzervezetiElem* és az *Ügyintéző* között EGY-SOK kapcsolat áll fenn, miszerint egy szervezeti elemhez több ügyintéző is tartozhat. A GDPR terminológiájában az adatkezelési tevékenység ezen a szinten valósul meg. A következő felsorolás a *FelelősHolder* viselkedését mutatja be.

1. CREATE – Az ügyintézési folyamat indulásakor létre kell hozni egy-egy FelelősHolder-t az ügyintézésért felelős *Ügyintéző* és *SzervezetiElem* modellezéséhez.

2. READ – Egy folyamatban lévő, illetve lezárt ügy vonatkozásában a *Felelős* aktív adatainak kinyerése történhet a *SzervezetiElem*-ből vagy az *Ügyintéző*-ből, illetve egy lezárt ügy esetén a *FelelősHolder*-ből.
3. UPDATE – Az egyes ügyintézési folyamatok sajátossága lehet, hogy a *Felelős* aktív adatainak módosítása már nincs hatással minden *FelelősHolder*-re. Az ügyintézésért felelős *SzervezetiElem* vagy *Ügyintéző* változásának hatására a *FelelősHolder*-t már nem feltétlenül kell megváltoztatni.
4. DELETE – Az *ÉrintettHolder* tervezési mintával analóg módon a teljes fizikai törlés is támogatható, de ügytípusonként is eljárhat az elektronikus ügyintézést biztosító szerv a *SzervezetiElem*-ek és az *Ügyintéző*-k vonatkozásában is.

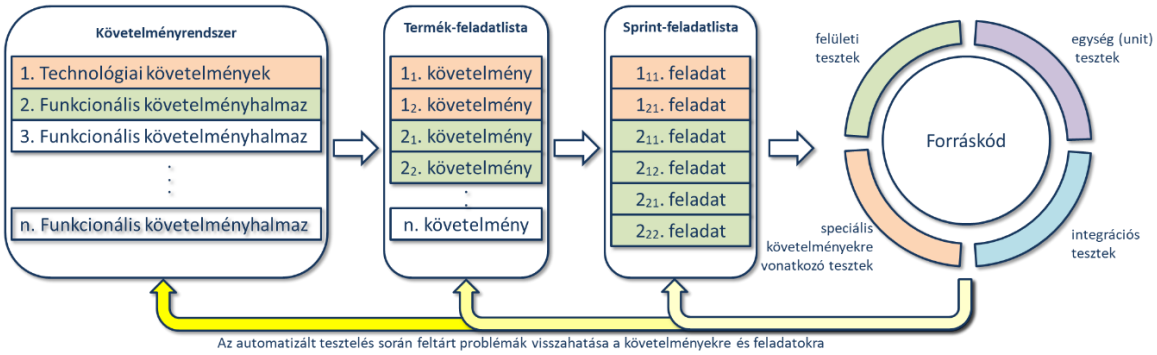
Az *FelelősHolder* tervezési minta alkalmazása lehetővé teszi az ügyintézési folyamat magas szintű támogatását a GDPR alapelveivel összhangban, különös tekintettel az ügyintézést végző természetes személyek adataira.

Technológiai háttér

A bemutatott tervezési minták használatához megfelelő színvonalú követelményelemzésre van szükség, ahol a használati esetek során tisztázásra kerülnek a speciális folyamatok a kapcsolattartás és belső folyamatok vonatkozásában. Ezek a különbségek határozzák meg a rendszerben definiálandó *Holder* objektumok viselkedését. A specifikáció megléte önmagában nem garantálja, hogy a tervezési minták sikeresen alkalmazhatók, mert törékeny logikai kapcsolatok alakulhatnak ki a tervezett informatikai rendszer adatmodelljében és adatbázisában. Ennek oka, hogy az adatkezelési tevékenységhez köthető *Érintett*-, *Ügyfél*- és *FelelősHolder*-ek bonyolult topológiát képezhetnek. Egy összetett adatmodellel rendelkező informatikai rendszer esetén a változáskezelés is problémás lehet, ha nincs meg a megfelelő technológiai háttér.

Célszerű lehet ebben az esetben a követelményelemzés és a szoftverfejlesztés támogatásához a *Military Scrum* [5; 178-180 o.][7; 215-220 o.][7; 235-242 o.] szoftverfejlesztési módszertan választása. A módszer a *Scrum* [8] szoftverfejlesztési módszertan továbbfejlesztett, katonai alkalmazáshoz kialakított változata, amely dokumentációs technikákat és fejlesztési módszereket ötvöz a megbízható, kiváló minőségű szoftverek előállítása céljából. A követelményelemzést támogató dokumentációs sablonok lehetővé teszik a jogszabályi, szervezeti és egyéb követelmények követelményhalmazokba történő szervezését. A fejlesztés során megkövetelt szerteágazó és magas szintű tesztlefedettség segítségével megvalósítható az evolúciós szoftverfejlesztés [5; 176-177 o.], így a kialakított informatikai rendszer képes adaptálódni a követelmények folyamatos változásához, ebben az esetben képes a kialakított *Holder*-ek helyes viselkedését garantálni a használati esetek tükrében.

Az Általános Adatvédelmi Rendelet vonatkozásában ez azt jelenti, hogy a *Military Scrum* alkalmazásával a GDPR alapelvek beépíthetők a követelményrendszerbe és a tesztforgatókönyvek kialakítása során a szoftver alkalmazója és a szoftverfejlesztő mérlegelhet az adatkezelési folyamatok kialakítása során. Így csak az adott adatkezelési tevékenységhez szükséges adatok kerülhetnek be az *ÉrintettHolder*-ekbe. A módszertan alkalmazható az elektronikus ügyintézést biztosító szervek informatikai rendszereinek kialakításakor is. Az ügyintézési folyamatok tervezése alatt a *Holder* objektumok a biztonságos és folyamatos ügyintézést támogatva kerülhetnek kialakításra.



8. ábra Military Scrum és az evolúciós szoftverfejlesztés folyamata (saját szerkesztés)

KÖVETKEZTETÉS

Az Európai Unióban és Magyarországon is számos rendelet, jogi szabályozás foglalkozik a kiberbiztonság témakörével – a témáról bővebben Gerevich János és Négyesi Imre kapcsolódó cikkeiből [9][10] is lehet tájékozódni. A fennálló hatályos dokumentumok közül az Általános Adatvédelmi Rendelet (GDPR) a jéghegy csúcsaként tűnik fel a kibertér biztonságáért folytatott küzdelemben, a GDPR alapelvei minden alkalmazási területen mérlegelendők: a *célhoz kötöttség*, az *adattakarékosság*, a *pontosság*, a *korlátozott tárolhatóság*, az *integritás* és a *bizalmas jelleg*. Az EU tagállamai megkapták a felhatalmazást arra, hogy kivételeket képezzenek de célszerű a jogszabályokban előírt adatkezelési tevékenységek során a GDPR elveinek figyelembe vétele és ezzel biztonságosabb és pontosabban működő informatikai rendszerek előirányzása. Az alapelveket nem csak a GDPR hatálya alá eső rendszerekben, hanem a kormányzati, illetve a védelmi szektor informatikai rendszereiben is megfontolandó alkalmazni, ahol a jogszabályi környezet ezt lehetővé teszi.

Az *ÉrintettHolder* és *FelelősHolder* tervezési minták lehetővé teszik a természetes személyek adataira vonatkozó létrehozási-, olvasási-, módosítási- és törlési műveletek konszolidált támogatását. A bemutatott megoldások támogatják az egy érintetthez/ügyfélhez tartozó párhuzamosan folyó adatkezelési tevékenységek konzisztenciájának fenntartását egy informatikai rendszeren belül tetszőleges CRUD műveletsorozat végrehajtásakor.

A *Holder* alapú tervezési minták alkalmazásának előfeltétele a tesztforgatókönyv alapú specifikáció és a megfelelő műszaki háttér. Amennyiben az informatikai rendszerek fejlesztése során a szoftver fejlesztője meg tudja valósítani az evolúciós szoftverfejlesztést, akkor az adatvesztés kockázata minimálisra csökken, cserében az érintettek személyes adatai egy adott adatkezelési tevékenység vonatkozásában naprakészen tarhatók, illetve indokolt esetben törölhetők. A szoftverfejlesztési feladatok elvégzéséhez egy lehetséges választás lehet a *Military Scrum* szoftverfejlesztési módszertan alkalmazása.

A védelmi szektor szemszögéből vizsgálva a problémát, úgy a tábori, mint a béke rendszerek vonatkozásában lehetséges a bemutatott tervezési minták használata, hierarchikus szervezeti felépítéssel rendelkező szervezetek is alkalmazhatják a megoldást. Tábori rendszerek esetében a *FelelősHolder*-ben megismert *SzervezetiElem* megfeleltethető a vezetési szinteknek, a kapcsolódó ügyintézők felfoghatók az adott vezetési szint alá tartozó alakulatoknak. A GDPR alapelveit betartva, szűkíthető a tárolandó és átadandó adatok köre, ezzel a katonai alkalmazású informatikai rendszer biztonsága szoftvertechnológiai oldalról növelhető.

Az Általános Adatvédelmi Rendelet a természetes személyek adatainak védelmére koncentrál, ugyanakkor alapelvei az informatika számos területén alkalmazhatók, beleértve a kormányzati és védelmi szektorokat is.

Felhasznált irodalom

[1] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról https://www.adatvedelmirendelet.hu/wp-content/uploads/Infotv.módosítás07.27..pdf (letöltve: 2018.12.01.)

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=HUA letöltve: (2018.12.03.)

[3] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól https://net.jogtar.hu/jogszabaly?docid=A1500222.TV (letöltve: 2018.12.03.)

[4] NÉGYESI IMRE: CHANGING ROLE OF THE INTERNET IN THE LIGHT OF AN INTERNATIONAL CONFERENCE (Az internet szerepének változása egy nemzetközi értekezlet tükrében) (Hadmérnök on-line, III. évfolyam (2008) 3. szám, 147-153. oldal, ISSN 1788-1919)

[5] GEREVICH J.: Az agilis szoftverfejlesztés alkalmazásának lehetőségei a Magyar Honvédség számára. In: Hadmérnök XII. 1. (2017) 170-181. o. http://hadmernok.hu/171_14_gerevich.pdf (letöltve: 2017. 04. 26.)

[6] GEREVICH J.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek. In: Hadmérnök XII. 3. (2017) 210-222. o. http://hadmernok.hu/173_19_gerevich.pdf (letöltve: 2017. 10. 15.)

[7] GEREVICH J., NÉGYESI I.: Híradó-informatikai fejlesztést támogató agilis dokumentációs módszerek - 2. rész In: Hadmérnök XIII. 1. (2018) 230-244. o. http://hadmernok.hu/181_18_gerevich.pdf (letöltve: 2018. 04. 30.)

[8] RUBIN K. S.: Essential Scrum. Ann Arbor, Michigan, USA, Pearson Education, Inc., 2013.

[9] GEREVICH J., NÉGYESI I.: A Military Scrum követelményelemző módszerének alkalmazása létfontosságú rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 3 (2018) 293-304. o.

[10] GEREVICH J. NÉGYESI I.: A Military Scrum szoftverfejlesztési módszertan alkalmazása létfontosságú infokommunikációs rendszerek fejlesztése során. In: Hadtudományi Szemle XI. 4 (2018) 72-82. o.