Gradus Vol 5, No 2 (2018) 110-116
ISSN 2064-8014

A GDPR ALKALMAZÁSÁBÓL ADÓDÓ INTÉZMÉNYI INFORMATIKAI ÉS JOGI FELADATOK

IT AND LAW TASKS IN THE INSTITUTION DURING THE USAGE OF GDPR

Miskolczi Ildikó[1] *PhD, LLM*

Közgazdasági, Pénzügyi és Menedzsment Tanszék, Gazdálkodási Kar, Neumann János Egyetem, Magyarország

Kulcsszavak:
GDPR
adatvédelem
személyes adat
adatkezelő
jogi és informatikai feladatok

Keywords:
GDPR
data protection
personal data
data management
legal and IT tasks

Cikktörténet:
Beérkezett 2018. augusztus 01.
Átdolgozva 2018. augusztus 31.
Elfogadva 2018. október 5.

Összefoglalás

2018. május 25. jelentős változásokat hozott Magyarországon is az adatvédelem területén. A 2018/679-es – rövid nevén GDPR – rendelet alapjaiban változtatja meg a természetes személyek személyes adatainak kezelési szabályait, hiszen a GDPR alkalmazásával a személyes adat fogalma rendkívül tág értelmezést kap, ugyanis bármiféle olyan adat személyes adatnak minősül, amely alkalmas a természetes személy azonosítására.

A cikk célja, bemutatni azokat az intézményi feladatokat, amelyek a GDPR-nak való megfelelés során az informatikai és a jogi feladatok körébe tartoznak, kezdve az adatvagyonleltár felvételétől az adatvagyon nyilvántartás kialakításán keresztül a hatásvizsgálati szempontok kialakításán túl a rendszertervezési, rendszerszervezési szempontokig.

Abstract

25th of May, 2018 brought significant changes in data protection in Hungary too. The 679/2018 - briefly called GDPR - regulation basically changes the rules for handling personal data of natural persons, because using the GDPR the concept of personal data is very broadly interpreted, since any data is considered to be personal data that is suitable for the identification of a natural person .

The purpose of the article is to present the institutional tasks that are part of the IT and legal tasks when complying with GDPR, ranging from the acquisition of inventory of data assets through the establishment of inventory of data assets, beyond the establishment of impact assessment criteria, to system design and system planning considerations.

1. Bevezetés

2018. május 25. jelentős változásokat hozott Magyarországon is az adatvédelem területén. A 2016/679-es[2] – rövid nevén GDPR – rendelet (továbbiakban: Rendelet) alapjaiban változtatja

[1] Kapcsolattartó szerző, tel.:+36 20 552 09 52
e-mail: miskolczi.ildiko@gk.uni-neumann.hu

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

meg a természetes személyek személyes adatai kezelésének szabályait, hiszen annak alkalmazásával a személyes adat fogalma rendkívül tág értelmezést kap. A Rendelet értelmében ugyanis bármilyen olyan adat személyes adatnak minősül, amely alkalmas a természetes személy azonosítására.

A Rendelet egyik központi alapelve, miszerint a természetes személyeknek joguk van a velük kapcsolatos adatkezelés bármely szakaszában a jogszerűséghez. A természetes személy fokozott jogosítványokkal (érintetti jogok) rendelkezik személyes adatai kezelése során illetve azokkal kapcsolatosan. Ezekből az érintetti jogokból adódóan az intézményi adatkezeléseknek is alkalmazkodniuk kell a rendelet előírásaihoz.

A Rendelet alkalmazása során több általános és speciális alapelvet kell figyelembe venni, ezekből kiemeltek az ÁTLÁTHATÓSÁG és az ELSZÁMOLTATHATÓSÁG alapelvei, melyek szerint az adatkezelőnek kell biztosítania az adatkezelése során, hogy a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végzi. (Alaptétel a rendelet szemléletében, miszerint az adat az érintett tulajdona, így rendelkezési joga van felette, az adatkezelés minden pillanatában tudnia kell (joga van tudni), hogy mikor, miért, mi történik az ő adataival.) Az átlátható adatkezelési eljárásban olyan jogi és informatika megfelelés biztosítására van szükség, mint:

- adatvagyonleltár felvétele
- adattisztítás elvégzése
- folyamatleírások elkészítése
- nyilvántartások létrehozása és folyamatos vezetése
- szabályzatok felülvizsgálata, létrehozása
- mintaszerződések felülvizsgálata, módosítása.

Az elszámoltathatóság elve azt jelenti, hogy az adatkezelő felelős az adatvédelmi elvek teljesüléséért, továbbá képesnek kell lennie az adatkezelés bármely szakaszában a megfelelés igazolására. Gyakorlatilag ezen elv teljesülése adja meg az adatkezelő központi szerepét az egész adatkezelés során, hiszen ő felel a

- jogszerű lebonyolításért és a vonatkozó adatvédelmi, adatbiztonsági szabályoknak való megfelelőségért, valamint
- képesnek kell lennie e megfelelés igazolására is (fontos a megfelelő dokumentálás, a szükséges lépések megtételének rögzítése és megfelelő ideig való tárolása).

Fontos tétel, miszerint a bizonyítási teher is megfordul jogsértés gyanúja esetén, azaz nem az érintettnek kell bizonyítania, hogy a jogai sérültek, hanem az adatkezelőnek, hogy ő minden szükséges intézkedést – ide értve a jogi és informatikai típusú intézkedéseket is – megtett, hogy a kezelt adatok ne sérüljenek, ne következzen be illetéktelen hozzáférés, incidens és az érintetti érdekek ne sérüljenek.

2. GDPR szemlélet: teher vagy lehetőség?

Bár a jogi „adaptáció”, a hazai GDPR-kompatibilis szabályozás területén sok teendő van még, hiszen csupán az Információs önrendelkezési jogról és az információs szabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info tv) legfontosabb módosításait fogadta el az elmúlt három hónapban a Parlament, mégis a Rendelet életbelépésével elindult egy új korszak a magyar jogban is az adatvédelem területén. Az ágazati, pontosító jogszabályok megjelenéséig (amelyek teljes egészeben megteremtik majd az összhangot egyes szakmai területek és a GDPR között) azonban közvetlenül a Rendeletből és az Info tv-ből adódó szabályok betartása kötelező egyformán minden jogalkalmazóra.

Azonban „Semmi ok a pánikra, az újdonságok nem tartalmaznak radikális változást a jelenleg hatályos hazai szabályokhoz képest, nehézséget okozhat azonban, ha az adatkezelő a kötelezettségeinek eddig csak módjával tett eleget.” [1].

3. A jogi és informatikai feladatok összhangja

A felkészülési időszak (utáni) feladatok több terület összehangolt munkáját jelentik a Rendelet jogszerű alkalmazása során. A jogi megfelelés biztosítása elengedhetetlen, de az informatikai biztonsági intézkedések megléte, alkalmazása is rendkívül fontos tényező. Az alkalmazás terén az ún. "harmadik láb" a human elem, hiszen általánosságban a jogalkalmazóktól, de konkrét ügyekben az adatkezelőktől, adatfeldolgozóktól és az érintettektől is elvárt a jogkövető magatartás.

Melyek tehát a legfőbb feladatok (a teljesség igénye nélkül, hiszen a cikk kereteit jóval meghaladja a valós feladatok sora), amelyekkel nem várhatunk az ágazati szabályok megjelenéséig? Fogalmazhatunk úgy, melyek azok az általánosan, minden adatkezelőre vonatkozó feladatok, amelyek a jogszerű adatkezelést biztosítják?

3.1. Készítsünk adatkezelési szabályzatot

Legelső és egyben legfontosabb feladat egy adatkezelési szabályzat megalkotása, amely a szervezetünkre szabottan standardizált formában tartalmazza az adatkezelés egyes eseteire érvényes előírásokat, eljárásokat tájékoztatásokat, formanyomtatványokat, a megfelelő jogi tájékoztatásokat.

Kis és középvállalkozások számára a Rendelet direktben nem írja elő adatkezelési szabályzat készítését – tehát, ha nincs ilyen, akkor a vállalkozás nem követ el mulasztást – csak nehezebben tudja igazolni a Rendeletnek való megfelelést. Az adatkezelési szabályzat készítése mellett több nyomós érv is felhozható.

Elsőként az „elszámoltathatóság" elvéből (5. cikk (2)) következik, hogy jó, ha a vállalkozás, szervezet rendelkezik adatkezelési szabályzattal. Amint azt korábban írtam, az elszámoltathatóság elve azt jelenti, hogy az adatkezelőnek képesnek kell lennie az adatvédelmi alapelveknek való megfelelés igazolására az adatkezelés bármely szakaszában. Az adatkezelési szabályzat a megfelelés alapdokumentuma, amely tartalmazza a megteendő intézkedéseket is.

Második érv, hogy az adatvédelmet be kell építeni a szervezet működési kultúrájába, a munkavállalókat ki kell képezni a jogszerű adatkezelésre – ezt a feladatot is megkönnyíti az adatkezelési szabályzat.

Végül, de nem utolsó sorban, az adatkezelési szabályzat az érintett személyek – munkavállalók, szerződés partnerek – tájékoztatását is szolgálja.

3.2. Készítsünk egy részletes adatkezelési tájékoztatót, útmutatót is

A fent említett adatkezelési szabályzat egy belső dokumentum, így ezt teljes terjedelmében és tartalmában nem célszerű nyilvánossá tenni, ezért ennek nyilvánosságnak szánt részét foglaljuk össze egy adatkezelési tájékoztatóban, amelyre az érintettek részére adandó minden egyes tájékoztatás során utalhatunk, mint amely részletesen tartalmazza a vonatkozó eljárásokat, szabályokat. Az útmutató lényeges elemei közé tartozik az adatkezelő valamint az adatfeldolgozók megnevezése, az adatvédelmi tisztviselő elérhetőségének megismertetése, valamint a szervezetben a lehetséges adatkezelési jogalapok nevesítése, az érintett részéről gyakorolható jogok, a szervezet által megtett adatbiztonsági intézkedések, valamint a jogorvoslati lehetőségek. Értelemszerűen a szervezetre vonatkozó speciális rendelkezéseket is megjeleníthetjük a tájékoztatóban. Ezt az adatkezelési tájékoztatót célszerű feltölteni a szervezet honlapjára, betöltve így az előzetes és folyamatos tájékoztatás funkcióját.

3.3. Munkaszerződési kikötéssel tegyük a munkavállalók kötelezettségével az adatkezelési szabályok betartását és érvényesítését

A szervezet minden munkavállalójával meg kell ismertetni az adatkezelési szabályzatot, elő kell írni részükre, hogy annak tájékoztatásait, formanyomtatványait munkavégzésük során, amikor más munkavállalók, ügyfelek, partnerek személyes adatait kezelik – érvényesítsék és alkalmazzák. Miután ez a munkaviszonyból eredő lényeges kötelezettség – erről minden munkavállalóval egy munkaszerződés-kiegészítést kell aláíratni. Lényeges adatbiztonsági intézkedés, hogy a személyes adatok kezelésével foglalkozó munkatársaktól a személyes adatok kezelésére titoktartási nyilatkozatot kell kérni. Ezt a Rendelet kifejezetten csak az

adatfeldolgozóknál írja elő – de minden adatkezelő alkalmazhatja, hiszen ez egy lényeges adatbiztonsági intézkedés.

3.4. Indokolt a munkavállalók részére külön képzést szervezni a személyes adatok jogszerű kezelése tárgyában

A téma aktuális is, fontos is. A Rendelet súlyos bírságszankciókat is tartalmaz, amely ösztönzőleg kell hogy hasson a megelőzésre, így a képzésre is. A képzés keretében ismertetésre kerülhet az adatkezelési szabályzat is. A belső képzések, tájékoztatások segítik a dolgozókat abban, hogy mindig naprakészek és jogkövetőek tudjanak maradni a napi munkavégzésük során, hiszen egy esetleges adatvédelmi incidens súlyos következményekkel járhat az adatkezelő, de az érintettek tekintetében is.

3.5. Új munkavállaló felvételekor hiánytalanul teljesítsük az adatkezelésre vonatkozó kötelezettségeket

Legegyszerűbb, ha az új munkavállalók esetében a munkaszerződésbe, kinevezésbe építjük be az adatkezelési kikötést, amely szerint a munkavállaló kijelenti, hogy a munkáltató adatkezelési szabályzatát megismerte, és annak rendelkezéseit a munkavégzés során alkalmazni köteles. Az adatbiztonsági részeként indokolt a munkavállalók részére titoktartási kötelezettséget előírni a személyes adatok kezelése vonatkozásában.

A munkavállaló részére a munkaszerződés megkötésekor tájékoztatást kell adni saját személyes adatai munkáltató általi kezeléséről és adatfeldolgozó részére történő átadásáról. E tájékoztatóval teljesíthető az a törvényi kötelezettség is, miszerint a munkáltatónak előzetesen tájékoztatnia kell a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak (pl. munkahelyi kamera alkalmazása, rendszerbe épített informatikai módszerek, folyamatok, internetfigyelés munkahelyi gépeken, hivatali gépjárművek GPS adatainak figyelése…). Ezek nem új szabályok, a Munka törvénykönyve írja elő ezeket már 2012 óta.

Adatfeldolgozó a saját munkavállalóival a személyes adatok kezelése tárgyában szintén köteles titoktartási nyilatkozatot aláíratni.

3.6. A régi munkaszerződéseket vizsgáljuk felül az adatkezelési kötelezettségek teljesítése szempontjából

Ajánlatos felülvizsgálni a már fennálló munkaszerződéseket is az előbbi pontban írt szempontok szerint.

A munkaszerződéseket ki kell egészíteni az adatkezelési kikötéssel, amely szerint a munkavállaló kijelenti, hogy a munkáltató adatkezelési szabályzatát megismerte, és annak rendelkezéseit a munkavégzés során alkalmazni köteles. Természetesen az adatkezelési szabályzatot a valóságban is meg kell ismertetni a „régi” munkavállalókkal is. Az adatbiztonsági részeként indokolt a munkavállalók részére titoktartási kötelezettséget előírni a személyes adatok kezelése vonatkozásában.

Adott esetben pótlólag a munkavállaló részére az adatkezelési szabályzat szerinti tájékoztatást kell adni saját személyes adatai munkáltató általi kezeléséről és adatfeldolgozó részére történő átadásáról csakúgy, mint ahogyan szükséges a munkavállalók előzetes tájékoztatása az ellenőrzésre szolgáló technikai eszközök alkalmazásáról az adatkezelési szabályzat alapján.

Az Adatfeldolgozó a saját „régi” munkavállalóival is köteles a személyes adatok kezelése tárgyában titoktartási nyilatkozatot aláíratni.

3.7. A szervezet által alkalmazott szerződési formulákba, és általános szerződési feltételekbe építsünk be az adatkezelési kikötést.

Ez értelemszerűen a szervezet által természetes személlyel vagy társas vállalkozás képviselőjével, kapcsolattartójával kötött szerződésre lesz alkalmazandó, függetlenül az adatkezelés jogalapjától.

A jogi személyekre – és a velük kötött szerződésekre nem terjed ki a Rendelet hatálya – azonban a jogi személyeket is természetes személyek képviselik, és az egyéb kapcsolattartóik is természetes személyek – az ő személyes adataik kezelésére tehát már vonatkoznak az adatvédelmi szabályok.

3.8. Ha adatfeldolgozónak minősül a szervezet, készítsünk adatfeldolgozási szerződést, vagy erre vonatkozó általános szerződési feltételeket, és szerezzük be a munkavállalók titoktartási nyilatkozatát.

Az adatfeldolgozónak garancianyújtási kötelezettsége van a megbízó adatkezelő felé, hogy a Rendelet szerinti adatvédelmi követelményeket az adatfeldolgozás során teljesíteni tudja. A garancia-nyújtási kötelezettség tartalmát a Rendelet ugyan nem tisztázza, de ennek teljesítéseként szolgálhat az adatfeldolgozó szerződéses kötelezettségvállalása.

Ezen adatkezelési kikötések – vagy önálló szerződésként, vagy általános szerződési feltételként – az adatkezelő és az adatfeldolgozó között meglévő vagy kötendő alapjogviszony szerződéséhez kapcsolódnak, annak kiegészítését, mellékletét képezik. Az alap megbízási szerződésben javasolt arról rendelkezni, hogy az „adatkezelési kikötéseket külön adatfeldolgozási szerződés tartalmazza, amely a megbízási szerződés melléklete.

A Ptk. rendelkezései szerint az általános szerződési feltétel tartalmát a másik féllel a szerződéskötést megelőzően meg kell ismertetni, és azt a másik félnek el kell fogadnia – azaz tehát ugyanúgy alá kell írni, mint egy egyedi szerződést [2].

Az adatfeldolgozók lényeges kötelezettsége, hogy beszerezzék munkavállalóik titoktartási nyilatkozatát a személyes adatok kezelése tárgyában.

Ha az adatfeldolgozó alvállalkozót vesz igénybe, ezt a megbízó adatkezelő hozzájárulásával teheti, és erre írásba foglalt szerződést kell kötni.

3.9. Készítsük el az adatkezelési tevékenységek nyilvántartását

A Rendelet bevezetője szerint a mikro-, kis- és középvállalkozások sajátos helyzetének figyelembevétele érdekében a 250 főnél kevesebb személyt foglalkoztató szervezetek esetében adatkezelési nyilvántartás vezetése alól mentesülnek. Van azonban egy olyan kivétel, amely az egész rendelkezést lerontja. A nem alkalmi jellegű adatkezelésre ezeknek a szervezeteknek is kell vezetnie az adatkezelési tevékenységek nyilvántartását. Márpedig a rendes működéshez kapcsolódó adatkezelések nem „alkalmiak.”

A Rendelet szerint az adatkezelési tevékenységek nyilvántartását az adatkezelőknek a saját adatkezelésükről kell vezetniük. Ez mellett az adatfeldolgozóknak kell vezetniük a más adatkezelő nevében végzett adatkezelési tevékenységük nyilvántartását is.

3.10. Tegyük meg a szükséges adatbiztonsági intézkedéseket

Lehetséges adatbiztonsági intézkedések:

- az informatikai rendszerek szoftveres védelme (tűzfal, vírusvédelem),
- hozzáférési szintek kialakítása és érvényesítése,
- az adathordozók – számítógépek, adattárolók, iratok, szerződések, bizonylatok, tároló helyiségek jelszóval történő valamint fizikai védelme, pl. zárható helyiségben.
- az adatkezeléssel foglalkozó munkatársaktól a személyes adatokra titoktartási nyilatkozat kérése - titoktartási kötelezettség magában foglalja azt is, hogy az ügyintéző nem hagyja elől, mások által megtekinthetően a feldolgozásra váró személyes adatokat tartalmazó iratokat, bizonylatokat,
- a személyesen használt informatikai eszközök, (személyi számítógép, háttértárak) jelszóval történő védelme, nem csak a rendszer indításakor, hanem pl. képernyőzár feloldásakor is,
- gondoljuk át a felhőalkalmazások igénybevételét, csak megfelelő minősítéssel rendelkező felhőtárhely-szolgáltatót vegyünk igénybe.

A „józan paraszti ész” elve alapján gondoljuk át, hogy vállalkozásunk munkafolyamataiban hol sérülhet az adatbiztonság, hol áll fenn a veszélye a személyes adatok véletlen vagy jogellenes megsemmisítésének, elvesztésének, megváltoztatásának, vagy jogosulatlan hozzáférésnek az esélye. Az így feltárt gyenge pontokat erősítsük meg. Ezzel megelőzhetjük az adatvédelmi

incidensek bekövetkezését, amelyekre - ha mégis bekövetkeznének - a Rendelet bejelentési és tájékoztatási, illetve nyilvántartási kötelezettséget ír elő.

3.11. Vizsgáljuk felül szervezetünk honlapját az adatkezelési eljárások és tájékoztatások jogszerűsége vonatkozásában

Az adatkezelési tájékoztatókat időnként frissíteni indokolt.

A hozzájárulásra szolgáló négyzeteket ne pipáljuk ki előre, mert ez a Hivatal álláspontja elveszi a hozzájárulás önkéntességét.

A cookie-k kezelésére szintén ajánlott tájékoztatót készíteni és a honlapon elérhetővé tenni a felhasználók számára.

Legyünk külön figyelemmel az internetszolgáltatónkkal kötött szerződésünkre is, a szerződésben a szolgáltató felé megfogalmazott biztonsági elvárásainkat, és a szolgáltató felelősségét feltétlenül fogalmazzuk meg.

3.12. Dolgozzunk ki tervet az adatkezelési incidensek kezelésére

Rendkívül fontos, hogy ne csupán az előzetes biztonsági intézkedéseket tegyük meg, és építsük be a rendszerünkbe, de legyen egy “akciótervünk” a bekövetkező adatvédelmi incidensek hatékony, gyors kezelésére, a gyors kárenyhítésre. Ennek meg is kell jelennie mind a szervezet adatkezelési szabályzatában, mind pedig az érintettek részére készült adatvédelmi tájékoztatóban, útmutatóban is.

3.13. Alkalmazzuk az álnevesítést

Az álnevesítés a személyes adatok olyan módon történő kezelése, amelyek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai valamint a szervezési intzékedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez azt a személyes adatot nem lehet kapcsolni.

4. Összefoglalás

„A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását…”[3].

„A 21. század elején a szervezetek nagy részének egyik legfőbb vagyona az adat. Azonban a személyes adat nem (elsősorban) a személyes adatot kezelő szervezet tulajdona, hanem az adott személyé, akire az vonatkozik. A természetes személyek azzal, hogy hozzájárulnak személyes adatiak kezeléséhez, a tulajdonjogot nem adják át automatikusan az adatkezelőknek és adatfeldolgozóknak. A személyes adat feletti rendelkezés joga továbbiakban is alapvetően az adat tulajdonosáé marad. Ezért is különösen nagy a szervezetek felelőssége akkor, mikor személyes adatokat kezelnek.

Bár a személyes adat tulajdonjoga és az afeletti rendelkezés joga nem az adatfeldolgozót illeti, de a megfelelő adatbiztonsági gyakorlatok és adatvédelmi eljárások kialakítása, és a vonatkozó előírásoknak való folyamatos megfelelés biztosítása, annak igazolása és bizonyítása azonban a személyes adatot kezelő szervezet terheli.

Az adatvédelem tudatosságot igényel minden szereplőtől, amelyet minden érintetti személyes adat kezelése során be kell tartani. Ennek érdekében nem elegendő szabályokat életbe léptetni, technológiai kontrollokat kialakítani, naplózni és tesztelni, magának a vállalati kultúrának is ösztönöznie kell a tudatos adatkezelésre vonatkozó gyakorlat kialakítását és alkalmazását” [4].

A 2018. május 25-én életbe lépett GDPR Rendelet és a magyar Info tv együttesen bár részletesen szabályozzák a szereplők jogait és kötelezettségeit valamint feladatait, mégis az

apróbb, ágazati részletszabályok kidolgozása, elfogadása, illetve majd a mindennapokba történő beépülése még várat magára.

Irodalomjegyzék

[1] Gyöngyösi Balázs: Kényes teher helyett üzleti előnyt jelenthet a GDPR megfelelő alkalmazása, Világgazdaság online, 2018. március 06.
https://www.vg.hu/gazdasag/masolat-kenyes-teher-helyett-uzleti-elonyt-jelenthet-gdpr-megfelelo-alkalmazasa-819515/
letöltés ideje: 2018. augusztus 17.

[2] Vékás Lajos: A Polgári Törvénykönyv magyarázatokkal, Wolters Kluwer Kft., 2013 ISBN: 9789632952796

[3] GDPR Preambulum

[4] Kihívások és lehetőségek a GDPR kapcsán, Deloitte, online
https://www2.deloitte.com/hu/hu/pages/ado/articles/a-gdprrol-reszletesen.html#
letöltés ideje: 2018. augusztus 10.

Felhasznált jogszabályok

[5] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről

[6] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[7] 2013. évi V. törvény a Polgári Törvénykönyvről