UNIVERSITAS SCIENTIARUM SZEGEDIENSIS

SZEGEDI TUDOMÁNYEGYETEM

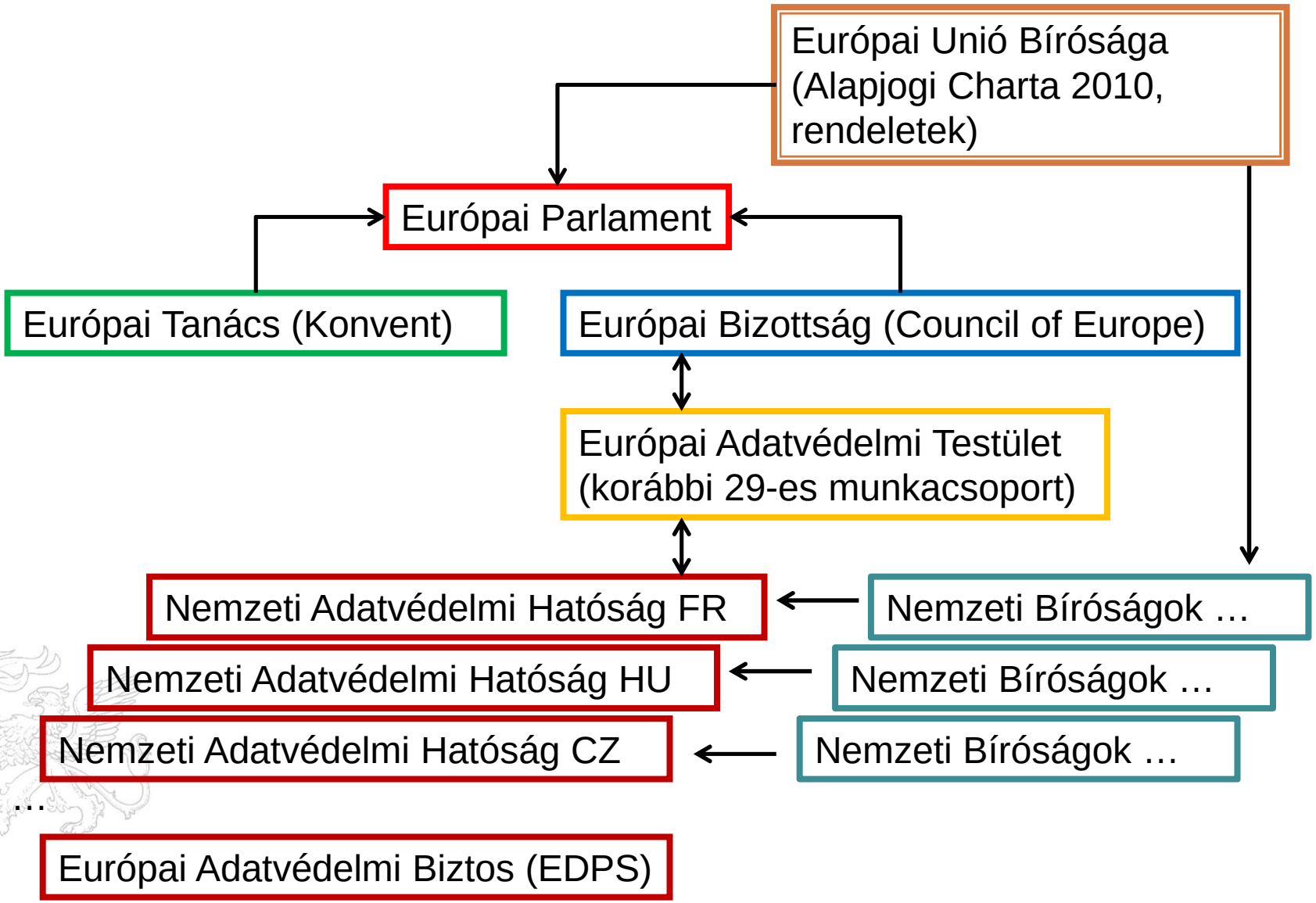
Szoftverfejlesztés Tanszék

Az Európai Unió általános adatvédelmi rendelete

Dr. Alexin Zoltán, PhD.
Szegedi Tudományegyetem, TTIK,
Szoftverfejlesztés Tanszék
H-6720 Szeged Árpád tér 2.
e-mail: alexin@inf.u-szeged.hu
http://www.inf.u-szeged.hu/~alexin

Előzmények

- Az Európai Unió Alapvető Jogok Chartája hatályba lép 2010. december 1.
- 8. cikk, A személyes adatok védelme
  - (1) Mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.
  - (2) Az ilyen adatokat csak tisztességesen és jóhiszeműen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogos okból lehet kezelni. Mindenkinek joga van ahhoz, hogy a róla gyűjtött adatokat megismerje, és joga van azokat kijavíttatni.
  - (3) E szabályok tiszteletben tartását független hatóságnak kell ellenőriznie.
- A 47. cikk szerint, akinek valamilyen jogát egy tagállamban megsértik, abban az államban bírósághoz fordulhat
- A probléma az volt, hogy a személyes adatok védelmére csak egy irányelve volt az EU-nak, amire nehezen lehetett pereket alapozni – bár ezért néha sikerült.


Európai Unió Bírósága
(Alapjogi Charta 2010,
rendeletek)
Európai Parlament
Európai Tanács (Konvent)
Európai Bizottság (Council of Europe)
Európai Adatvédelmi Testület
(korábbi 29-es munkacsoport)
Nemzeti Adatvédelmi Hatóság FR
Nemzeti Bíróságok …
Nemzeti Adatvédelmi Hatóság HU
Nemzeti Bíróságok …
Nemzeti Adatvédelmi Hatóság CZ
Nemzeti Bíróságok …
…
Európai Adatvédelmi Biztos (EDPS)

Idővonal

- Közmeghallgatás 2009. december 31-ig, adtunk le anyagot
- Konferencia a civil szféra számára Brüsszelben, 2010. július 2.
- Első verzió 2011. november 29.
- Az EU hivatalos lapjában megjelenik egy tervezet 2012. január 25.
- LIBE (Állampolgári Jogi, Bel- és Igazságügyi Bizottság) rendezte a beérkezett módosítási javaslatokat és publikálta 2012. dec 17-én,
- Az Európai Parlament szavazott számos javaslatról 2013. október 25-én.
- Az Európai Parlament első olvasatban elfogadja 2014. március 12.
- Az igazságügy miniszterek jóváhagyják a szöveget 2015. jún. 15.
- Az Európai Parlament és a Tanács elfogadja a végleges szöveget, 2015. dec. 15.
- Az EU Parlament elfogadja 2016. április 16.

A legfontosabb változások

- GDPR (General Data Protection Regulation)
- 2016. május 25-én hatályba lépett a 2016/679. számú EU rendelet és a 2016/680. számú ajánlás,
- 2018. május 25-én megszűnik a 95/46/EK számú adatvédelmi irányelv és akkortól kell alkalmazni az új 2016/679. rendeletet,
- Minden tagállamban azonos formában,
- Európai Adatvédelmi Testület, felügyeli a nemzeti hatóságok munkáját, lesz jogalkotási lehetősége,
- Az állami szféra adatkezelése „közérdekű adatkezelés” lesz, jogorvoslattal és tiltakozási lehetőséggel,
- Megjelenik a korlátozások nélküli „jogos érdekből” történő adatkezelés (Opinion 06/2014 on the notion of legitimate interests, WP217_en.pdf, 29-es munkacsoport, C-468/10, C-469/10 ügyek)
- Sok adminisztratív kötöttség: kötelező tájékoztatás, széleskörű tiltakozás, „felejtés joga”, egészségügyben kötelező előzetes hatásvizsgálat.

Személyes adatok fogalma

- A 2016/679. rendelet (26) preambuluma szerint:
  - Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, **azonosítható természetes személyre vonatkozó adatnak** kell tekinteni. Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, …, és a technológia fejlődését. Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.

A pszeudonim adatok - személyesek

- 11. cikk:
- Azonosítást nem igénylő adatkezelés
  - (1) Ha azok a célok, amelyekből az adatkezelő a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintettnek az adatkezelő általi azonosítását, az adatkezelő nem köteles kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen e rendeletnek.
  - (2) Ha az e cikk (1) bekezdésében említett esetekben **az adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet**, erről lehetőség szerint őt megfelelő módon tájékoztatja. **Ilyen esetekben a 15–20. cikk nem alkalmazandó, kivéve, ha az érintett abból a célból, hogy az említett cikkek szerinti jogait gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.**

Egészségügyi adatok kezelése

- A 2016/679. rendelet (52) preambuluma szerint:
  - A személyes adatok különleges kategóriáira vonatkozó adatkezelési tilalomtól való eltérés szintén megengedhető, ha erről az uniós vagy tagállami jog rendelkezik, és ha arra megfelelő garanciák mellett kerül sor a személyes adatok és más alapvető jogok védelme érdekében, **ha ez valamely közérdeken alapul**, így különösen a foglalkoztatási jog és **a szociális védelmi jog területén, a nyugdíjakat is beleértve, valamint a népegészség-védelem, a nyomonkövetési és riasztási célok, a fertőző betegségek és más súlyos egészségügyi veszélyek megelőzése**, valamint az ellenük való védekezés érdekében végzett személyesadat-kezelés esetében. Ezekre az eltérésekre egészségügyi célokból – köztük a népegészségüggyel és az egészségügyi szolgáltatások irányításával kapcsolatos célokból – kerülhet sor, különösen annak biztosítása érdekében, hogy az egészségbiztosítási rendszer szolgáltatásaival és juttatásaival kapcsolatos igények rendezésére szolgáló eljárások magas szintűek és költséghatékonyak legyenek, továbbá a közérdekű archiválás céljából …

Kötelező adatkezelés vs. közérdek

- A 2016/679. rendelet szerint:
- 6. cikk Az adatkezelés jogszerűsége
  - (1) A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:
  - …
  - c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
  - d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
  - **e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;**
  - f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Különleges adatok kezelése

- A 2016/679. rendelet szerint:
- 9. cikk, A személyes adatok különleges kategóriáinak kezelése
  - (1) A faji vagy etnikai származásra, …, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése **tilos**.
  - (2) Az (1) bekezdés nem alkalmazandó abban az esetben, ha:
    - a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez …;
    - …
    - h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, … a (3) bekezdésben említett feltételekre és garanciákra figyelemmel;
    - i) az adatkezelés a népegészségügy területét érintő olyan **közérdekből szükséges**, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, … ;

NJSZT-OBSz, Az egészségügyi intézményi adatok védelme, 2016. június 10., Balatonalmádi

Alapvető jogok chartája

- 3. cikk, A személyi sérthetetlenséghez való jog
- (1) Mindenkinek joga van a testi és szellemi sérthetetlenséghez.
- (2) Az orvostudomány és a biológia területén különösen a következőket kell tiszteletben tartani:
  - a) az érintett személy szabad és tájékoztatáson alapuló beleegyezése a törvényben megállapított eljárásoknak megfelelően,
  - b) az eugenikai, különösen az egyedkiválasztást célzó gyakorlat tilalma,
  - c) az emberi test és részei ekként történő, haszonszerzési célú felhasználásának tilalma,
  - d) az emberi lények szaporítási célú klónozásának tilalma.

- Magyarországon problémás az (1) bekezdés és a (2) bekezdés a) pontja.

Jog a törléshez (felejtéshez)

- 17. cikk, A törléshez való jog („az elfeledtetéshez való jog”)
- (1) Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, … ha az alábbi indokok valamelyike fennáll:
  - …
  - c) az érintett a 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
- (3) Az (1) és (2) bekezdés nem alkalmazandó, amennyiben az adatkezelés szükséges:
  - …
  - c) a 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;
  - d) a 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az … említett jog **valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést**;

A tiltakozás joga

- 21. cikk, A tiltakozáshoz való jog
  - (1) Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a **6. cikk (1) bekezdésének e) vagy f) pontján alapuló kezelése ellen**, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy **az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek** az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.
  - (6) Ha a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

A beépített adatvédelem

- 25. cikk, Beépített és alapértelmezett adatvédelem
  - (1) Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.
  - (2) Az adatkezelő megfelelő **technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek**. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. **Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.**

Kötelező incidens-bejelentés

- 33. cikk, Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak
  - (1) Az adatvédelmi incidenst az adatkezelő indokolatlan **késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott**, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.
- 34. cikk, Az érintett tájékoztatása az incidensről
  - (1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
  - (4) Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a (3) bekezdésben említett feltételek valamelyikének teljesülését.

Adatvédelmi hatásvizsgálat

- 35. cikk, Adatvédelmi hatásvizsgálat
  - (1) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor **az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.** …
  - (2) Ha van kijelölt adatvédelmi tisztviselő, az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát köteles kikérni.
  - (3) Az (1) bekezdésben említett adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:
    - …
    - **b) a 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy**
    - c) nyilvános helyek nagymértékű, módszeres megfigyelése.

Jogorvoslati lehetőségek

- Nemzeti adatvédelmi hatóság határozatban kötelezheti az adatkezelőket
- A nemzeti adatvédelmi hatóságok együttműködnek az EU Adatvédelmi Testülettel és harmonizálják a jogalkalmazást
- Az adatvédelmi hatóság intézkedése ellen jogorvoslatért a nemzeti bírósághoz lehet fordulni
- Ha volt az EU Adatvédelmi Testületnek állásfoglalása, akkor azt a nemzeti bíróságnak meg kell küldeni
- A nemzeti bíróság kérheti az EU Adatvédelmi Testület állásfoglalásának felülvizsgálatát az EUB-tól a TFEU szerződés 263. cikke alapján
- A polgárok előzetes döntéshozatali eljárást kérhetnek a bírósági eljárás során EUB-tól a TFEU szerződés 267. cikk alapján

Összefoglalás

- Egészségügyi intézményekben kötelező adatvédelmi felelőst alkalmazni (eddig is így volt),
- Hatásvizsgálatot kell készíteni,
- Az egészségügy jogalapja a kifejezett hozzájárulás lesz, vagy a közérdek [kivéve a járványveszélyt, népegészségügyi monitorozást],
- A népegészségügyet nem lehet kiterjesztően értelmezni és gyakorlatilag kutatást végezni népegészségügy címén,
- Minden egyes adatkezelés előtt kötelező lesz tájékoztatást adni, minden egyes célról, és minden egyes célnál meg kell jelölni jogalapot,
- Ha nem az érintettől szerzik meg az adatokat, akkor kötelező lesz a tájékoztatás [levélben 30 napon belül],
- A kutatás jogalapja az önkéntes hozzájárulás lesz, kivételes esetben a magasabb rendű közérdek – de utóbbi esetben is lesz tiltakozási lehetőség,
- Minden esetben lehet majd tiltakozni és pert indítani adattörlésért, kivéve talán a KSH (nemzeti statisztikai) adatkezelést,
- Az adatok törléséért is lehet majd pert indítani.

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
SZEGEDI TUDOMÁNYEGYETEM
Szoftverfejlesztés Tanszék

Köszönöm a figyelmet!