Nemzeti Adatvédelmi és Információszabadság Hatóság

Az adatvédelem új rendje

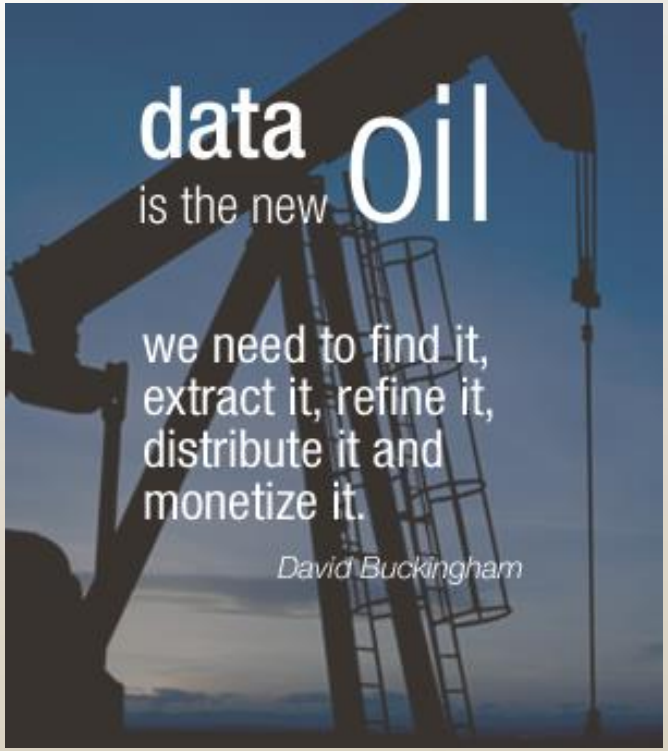
A GDPR néhány újdonságának rövid bemutatása

dr. Osztopáni Krisztián


DATA
is the new oil

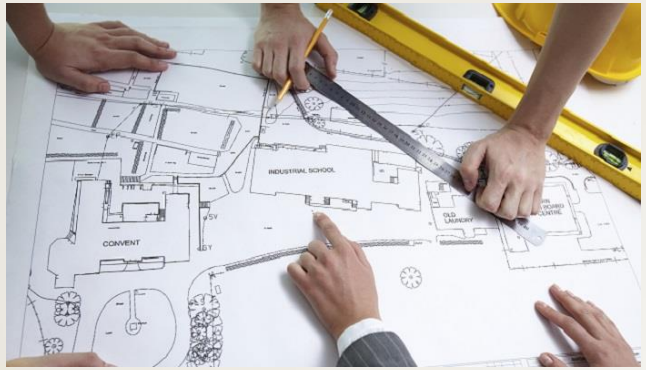

DATA
IS THE NEW OIL
but do you have the resource to refine it?

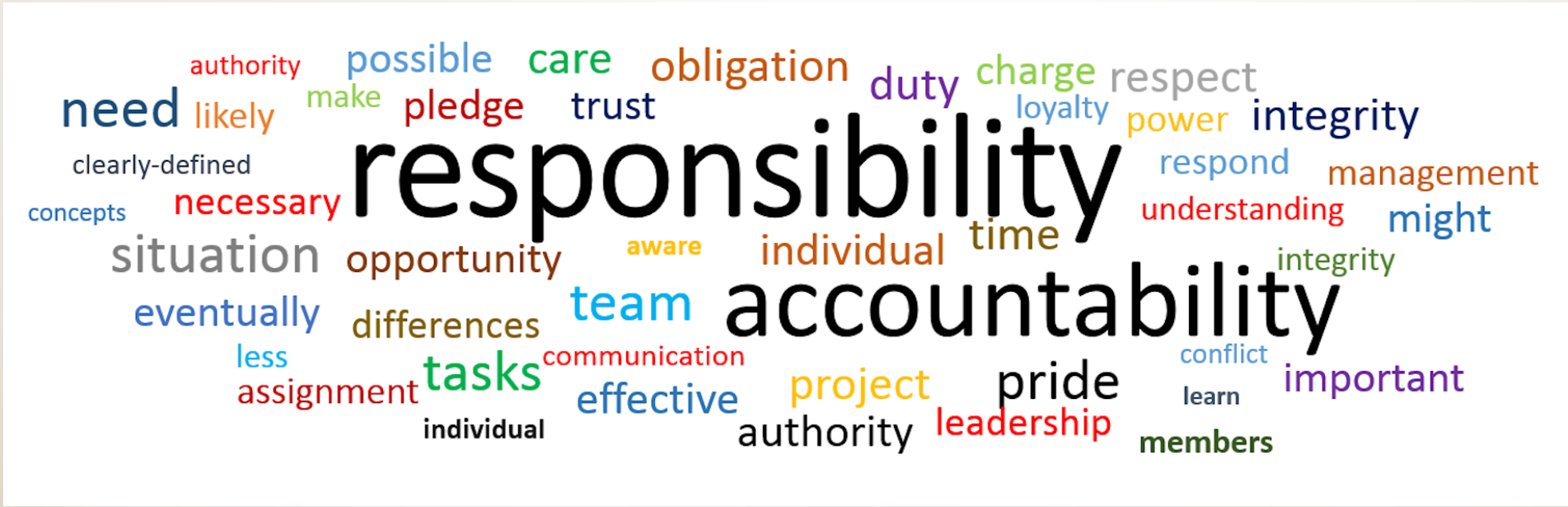

data is the new oil
BIG DATA
CLOUD
AZURE
DEVELOPERS
APPS
PLATFORM
WEB
DEVICES
PEOPLE


data
is the new oil
we need to find it,
extract it, refine it,
distribute it and
monetize it.
David Buckingham


DATA IS
THE NEW OIL
The New Generation of Leaders in Business Analytics

Nemzeti Adatvédelmi és
Információszabadság Hatóság




authority
possible
care
obligation
duty
charge
respect
need
likely
make
pledge
trust
loyalty
power
integrity
responsibility
clearly-defined
respond
management
concepts
necessary
understanding
might
time
situation
opportunity
aware
individual
integrity
accountability
eventually
team
differences
less
communication
conflict
tasks
project
pride
important
assignment
effective
learn
individual
authority
leadership
members

Nemzeti Adatvédelmi és Információszabadság Hatóság

1. Elszámoltathatóság elve

A GDPR „szuperelve”, amely az adatkezelőkkel szembeni legfőbb elvárást testesíti meg [GDPR 5. cikk (2) bekezdés].

1. **Az adatkezelőknek meg kell felelniük az alapelveknek.**

2. **Az adatkezelőknek bizonyítani kell tudniuk azt, hogy megfelelnek ezeknek az alapelveknek.**

3. **Amennyiben az adatkezelőknek „mozgásteret” biztosít a GDPR, akkor képesnek kell lenniük annak bizonyítására, hogy az adatkezelésük összhangban van a GDPR rendelkezéseivel.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

1. Elszámoltathatóság elve

Az elszámoltathatóság elvét elősegítő mechanizmusok a GDPR-ban:

- **adatvédelmi tisztviselő kijelölése**
- **belső adatvédelmi nyilvántartás vezetése**
- **adatfeldolgozói szerződések kötelező tartalmi elemei**
- **adatvédelmi hatásvizsgálat elvégzése és előzetes konzultáció a felügyeleti hatósággal**
- **valamely adatkezelés vagy termék, szolgáltatás tanúsítása**

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az adatkezelés megtervezése

Egy adatkezelés megtervezése során elsődlegesen az alábbi alapvető kérdéseket kell megválaszolnia egy adatkezelőnek:

1. *Ki?* — Ki az adatkezelő, adatfeldolgozó?
2. *Miért?* — Milyen adatkezelési célból?
3. *Milyen alapon?* — Mi az adatkezelés jogalapja?
4. *Mit?* — Milyen személyes adatot?
5. *Meddig?* — Mennyi ideig tart a személyes adatok kezelése?
6. *Milyen módon?* — Milyen adatbiztonsági körülmények mellett?

Nemzeti Adatvédelmi és Információszabadság Hatóság

2. Az adatkezelés megtervezése

A megfelelő jogalapok kiválasztásában nagyobb a mozgástere az adatkezelőnek, mint korábban az Infotv. alapján.

- **Hozzájárulás kérése vagy érdekmérlegelés jogalapjának alkalmazása, így különösen a profilozás esetén?**

- **Mennyiben különbözik egymástól az eredeti adatkezelés és a tervezett új adatkezelés? [GDPR 6. cikk (4) bekezdés]**

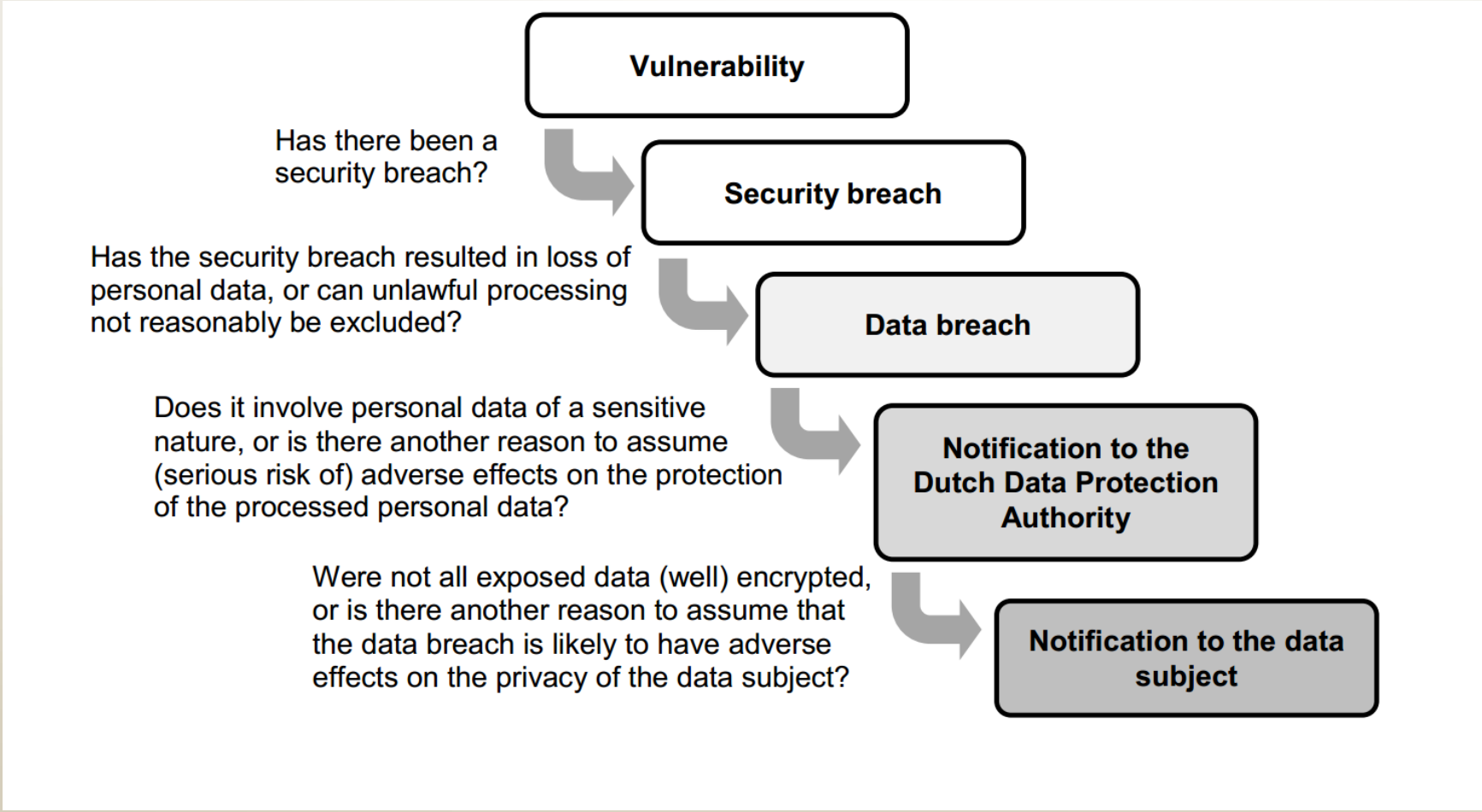
- **Az adatkezelő gyakorlatában lehet-e alkalmazni „a szerződéskötés” jogalapját? [GDPR 6. cikk (1) bekezdés b) pont]**

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

Infotv. [3. § 26. pont]	GDPR [4. cikk 12. pont]
A jogosulatlan - hozzáférés - megváltoztatás - továbbítás - nyilvánosságra hozatal - törlés - megsemmisítés Valamint a véletlen - megsemmisülés - sérülés	Véletlen vagy jogellenes (jogosulatlan) - hozzáférés - megváltoztatás - közlés - törlés - megsemmisítés

3. Adatvédelmi incidensek



Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

Példa a sebezhetőségre („vulnerability”):

> ***„Ezen a portálon* [www.ssllabs.com] *a shop.bkk.hu oldal 2017. július 21-én pénteken F osztályzatot kapott. A Qualys teszteredménye arra utal, hogy a BKK szervere sérülékeny lehet a DROWN típusú támadással szemben, és ezen kívül még más hibákat is találni véltek a BKK portálján.”***
>
> ***http://index.hu/tech/2017/07/21/a_bkk_webshopja_biztonsagos/ 2017. július 21., Index.hu***

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek:

- **a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,**
- **a személyazonosság-lopást vagy a személyazonossággal való visszaélést,**
- **a pénzügyi veszteséget,**
- **a jó hírnév sérelmét,**
- **a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

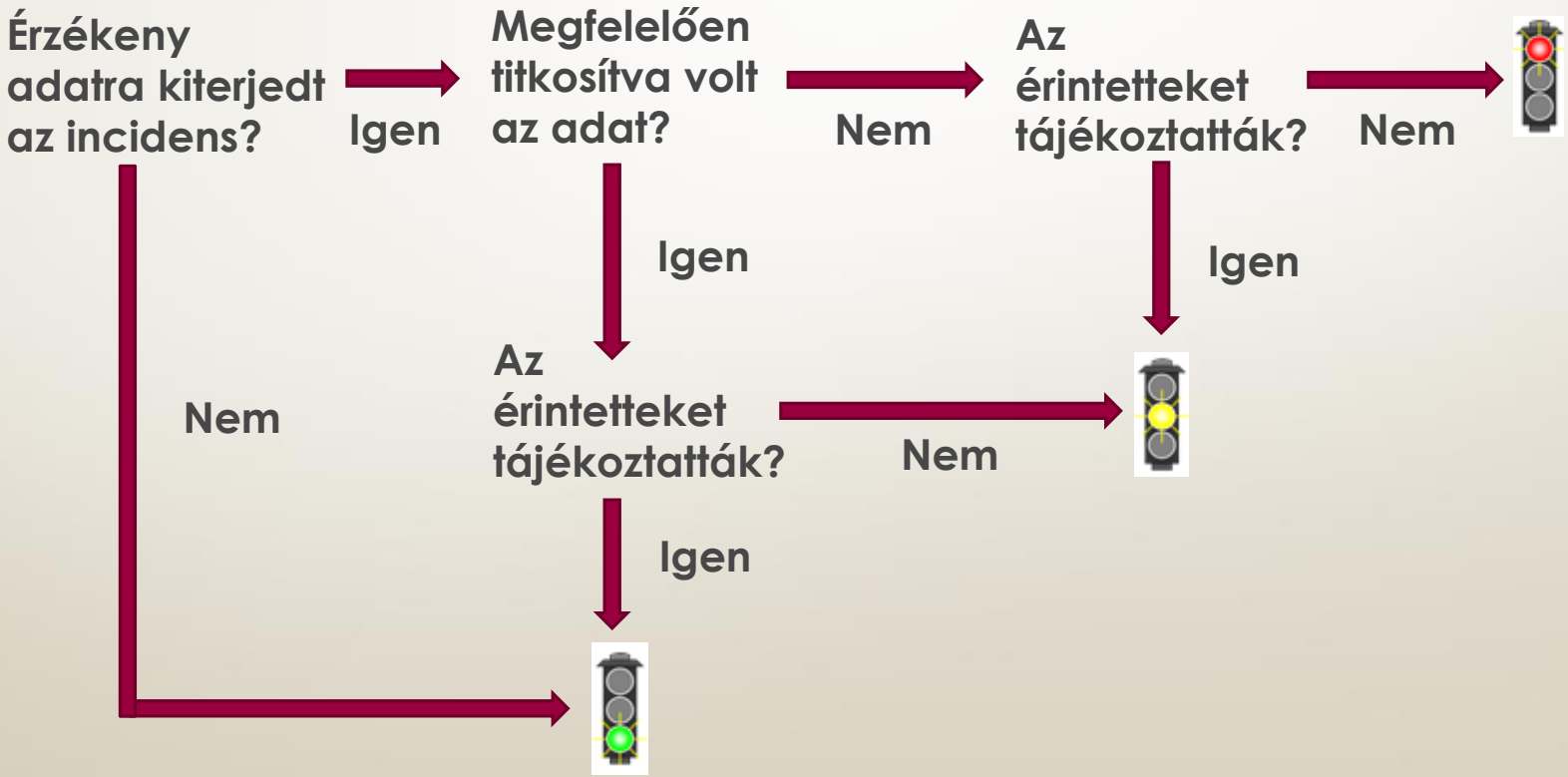
3. Adatvédelmi incidensek

„Érzékeny adatok”: ezen személyes adatokat érintő incidensek vélhetően kockázatot jelentenek a természetes személyek jogaira, szabadságaira:

- a különleges adatok
- az érintett pénzügyi helyzetére vonatkozó adatok (például tartozás)
- az érintett társadalmi megbecsülésére kiható adatok (például játékszenvedély, rossz iskolai eredmények)
- felhasználónevek és jelszavak
- a személyiséglopásra alkalmas adatok (például okmánymásolat)

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek



Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

NAIH-559/2013/H. számú ügy

2012. október 13-án nyilvánossá vált, hogy egy török hackercsoport feltörte a www.3d.pepsi.hu promóciós internetoldalt, és több mint 50.000 felhasználó személyes adatát (név, e-mail cím, telefonszám, születési dátum, a település neve, és a belépéshez használt jelszó) lopták el.

Az ismeretlen tettesek globalizáció- és USA-ellenes üzenete alapján arra lehet következtetni, hogy a támadás célpontjai multinacionális amerikai cégek voltak, mint a PEPSI, amelynek a FÁÜ Zrt. is az egyik leányvállalata.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

Az ötvenezer fős érintetti körből 695 fő esetében az e-mail fiók jelszava is kikerült a rendszerből. Ők voltak veszélyeztetettebbek, mivel harmadik személyek a közzétett jelszóval visszaélve e-mail fiókba vagy akár azonos jelszóval védett egyéb személyes felületükre is beléphettek.

Ennek a személyi körnek kétkörös e-mail üzenetet, valamint SMS üzenetet küldött ki az adatkezelő, egyúttal felhívták a fogyasztók figyelmét a jelszó megváltoztatására a visszaélések elkerülése érdekében.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

A FÁÜ Zrt. ezen túlmenően a válságkezelési intézkedései keretében:

- válságkezelő csoport felállításáról gondoskodott,
- a fogyasztók megkeresése érdekében telefonos ügyfélszolgálatokat állítottak fel,
- rendőrségi feljelentést tettek a BRFK Gazdaságvédelmi Főosztályán,
- továbbá az érintett hatóságokkal felvették a kapcsolatot.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

Az ellopott és illegálisan közzétett személyes adatok törlése érdekében a FÁÜ Zrt. felvette a kapcsolatot azoknak a honlapoknak (pastebin.com; bindrand.com; pastemine.com; hacktalk.com) az adminisztrátoraival, ahol az adatok közzétételre kerültek.

A hacktalk.net kivételével az adatokat eltávolították a honlapokról.

Nemzeti Adatvédelmi és Információszabadság Hatóság

3. Adatvédelmi incidensek

A hacktalk.net honlap számos megkeresés után sem vette le az adatokat (9 hónapig volt fenn az adatbázis), ezért a FÁÜ Zrt. hivatalos levélben fordult az adott honlap internetes adatbázisban számukra elérhető regisztrálójához, a WhoisGuardhoz a szükséges intézkedések megtétele iránt.

A FÁÜ Zrt. továbbá arról tájékoztatta a Hatóságot, hogy amennyiben a megkeresésük nem vezet eredményre, úgy az ICANN egységes domain jogvita-kezelési szabályzatára hivatkozva panasszal fordulnak az illetékes USA-beli WIPO szervezethez.

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. A felügyeleti hatóságok eljárása

Határon átnyúló egy adatkezelés, ha:

- **egynél több tagállamban van tevékenységi hely és több tagállamban végzik az adatkezelést, vagy**
- **egyetlen tevékenységi hely van, ugyanakkor az adatkezelés jelentős mértékben kihat egynél több tagállamban levő érintettekre.**

Fő felügyeleti hatóság: a tevékenységi központ szerinti hatóság.

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. A felügyeleti hatóságok eljárása

Minden felügyeleti hatóság jogosult a hozzá benyújtott panaszok kezelésére (függetlenül attól, hogy van-e fő felügyeleti hatóság), ha

- **az ügy tárgya kizárólag egy, a tagállamában található tevékenységi helyet érint,**
- **vagy ha kizárólag a tagállamában érint jelentős mértékben érintetteket.**

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. A felügyeleti hatóságok eljárása

Ilyenkor értesíteni kell a fő felügyeleti hatóságot, amely dönthet úgy, hogy nem veszi magához az ügyet, és az a felügyeleti hatóság folytassa le az eljárást, akinél a panaszt benyújtották.

Ugyanakkor olyan döntést is hozhat, hogy az ügyet „érintett felügyeleti hatóságokkal" közösen, együttműködési eljárásban vizsgálják ki a panaszt.

Az érintett felügyeleti hatóságoknak konszenzusra kell jutni a konkrét panasz vizsgálata során, mindenki egyetértsen a döntéstervezettel.

Nemzeti Adatvédelmi és Információszabadság Hatóság

4. A felügyeleti hatóságok eljárása

Érintett felügyeleti hatóság:

a) az adatkezelő vagy az adatfeldolgozó a felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel;

b) az adatkezelés jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy

c) panaszt nyújtottak be az említett felügyeleti hatósághoz.

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Előzetes tájékoztatás követelménye

„Különös jelentőséggel bír a tájékoztatás módja (egyszerű, zsargon használata nélküli, érthető, figyelemfelkeltő szövegben) annak értékelésekor, hogy a hozzájárulás »tájékozott«-e. A tájékoztatás módját a tartalomhoz kell igazítani:
a rendszeres/átlag felhasználó számára érthetőnek kell lennie.”

Adatvédelmi Munkacsoport 15/2011. számú Vélemény

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Előzetes tájékoztatás követelménye

„Minél összetettebb az adatkezelés, annál nagyobb az elvárás az adatkezelővel szemben. Minél nehezebbé válik az átlagpolgár számára átlátni és megérteni az adatkezelés valamennyi elemét, annál nagyobb erőfeszítéseket kell tennie az adatkezelőnek annak bizonyítása érdekében, hogy a hozzájárulás megszerzése konkrét és érthető tájékoztatáson alapult.”

Adatvédelmi Munkacsoport 15/2011. számú Vélemény

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Előzetes tájékoztatás követelménye

A 15/2011. számú Véleményben kifejtettek normaszöveggé váltak, minthogy szerepelnek a GDPR 12. cikk (1) bekezdésében:

> ***„Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó (…) tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa (…)”.***

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Előzetes tájékoztatás követelménye

A GDPR 13. cikke határozza meg az előzetes tájékoztató követelményeit abban az esetben, ha a személyes adatokat az érintettől gyűjtik:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól
- az érintettnek az a joga, hogy a hozzájárulását bármely időpontban visszavonhatja
- szerződéses kapcsolat létrejöttéhez szükséges-e a személyes adatok megadás, mi a következménye a hozzájárulás elmaradásának
- automatizált döntéshozatal (profilalkotás) logikája, hatásai az érintettre

Nemzeti Adatvédelmi és Információszabadság Hatóság

5. Előzetes tájékoztatás követelménye

A GDPR 13. cikk (3) bekezdése alapján az előzetes tájékoztatás követelményeit nem kell alkalmazni, „*ha és amilyen mértékben az érintett már rendelkezik az információkkal*.”

Önmagában az, hogy a formanyomtatványon szerepelt valamilyen tájékoztatás, akkor ez csak részben nem elegendő, ha nem felel meg a GDPR 13. cikk (1)-(2) bekezdése szerinti tartalmi követelményeknek.

Nemzeti Adatvédelmi és Információszabadság Hatóság

6. A bírságkiszabás szempontjainak rögzítése

GDPR 83. cikk (2) bekezdése alapján figyelembe kell venni például:

- a jogsértés jellege, súlyossága és időtartama, a jogsértés szándékos vagy gondatlan jellege
- az adatkezelés jellege, célja, a jogsértéssel érintett személyes adatok kategóriája
- az érintettek száma, és az általuk elszenvedett kár mértéke
- az adatkezelő vagy az adatfeldolgozó részéről az érintettek által elszenvedett kár enyhítése érdekében tett bármely intézkedés, továbbá ők maguk bejelentették-e a jogsértést

Nemzeti Adatvédelmi és Információszabadság Hatóság

Köszönöm a figyelmet!

dr. Osztopáni Krisztián
vizsgáló, NAIH

osztopani.krisztian@naih.hu