



AZ ADATVÉDELMI HATÓSÁG (NAIH) ELJÁRÁSAI

Sipos Győző –
IT Biztonsági Auditor, CISA, CDPSE



AZ ADATVÉDELMI HATÓSÁG (NAIH) ELJÁRÁSAI

ROSSZINDULATÚ BEJELENTÉSEK KEZELÉSE, AVAGY A FAGYI VISSZANYAL



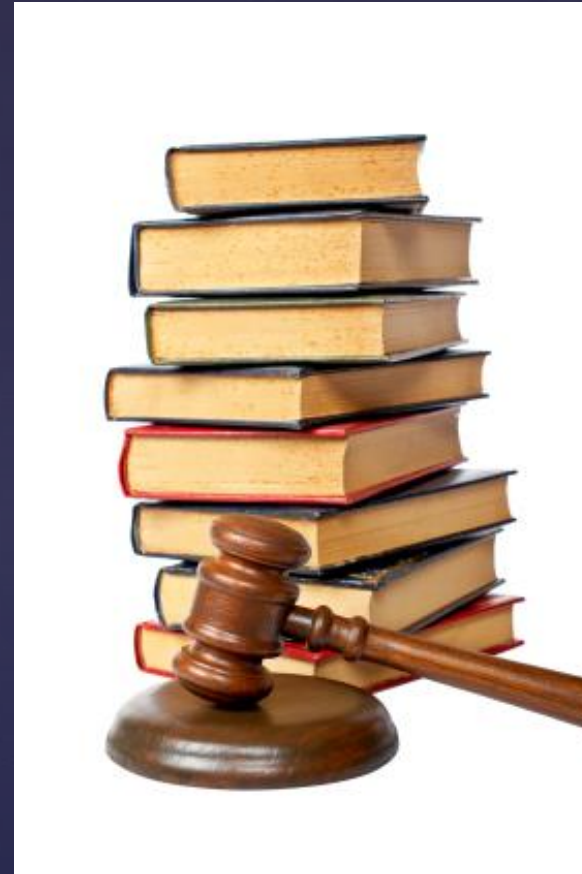
A MAI ÉTLAP

- A NAIH jogállása
- A NAIH feladatai
- Miért indulnak hatósági eljárások?
- Esetek a Nádor Rendszerház gyakorlatából
- Útravaló



Amiről talán hallottak... (2017)

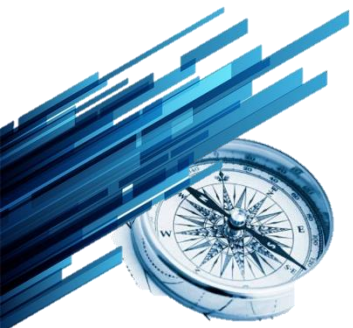
- Jön az EU GDPR!
 - Mi is ez?
- Kötelező!
 - Kinek is?
- Nagy szigor, bírságok!
 - Micsoda? Mennyi? Miért is?
- Jó ez nekünk?
 - IGEN!!!



A NAIH JOGÁLLÁSA

1. § (1) A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) önálló jogi személyiséggel rendelkező autonóm államigazgatási szerv, melynek feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése.

(2) Az (1) bekezdés szerinti tevékenysége ellátása során a Hatóság önállóan gyakorolja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) megállapított hatáskörét. A Hatóság független, kizárólag a törvényeknek alárendelten működik, számára feladatot csak törvény állapíthat meg. Feladatkörében nem utasítható, a feladatát más szervektől elkülönülten, befolyásolástól mentesen látja el.



A HATÓSÁG FELADATA, ALAPTEVÉKENYSÉGE

L2. § (1) A Hatóság feladatkörében az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) meghatározottak szerint

- a) bejelentés alapján vagy hivatalból vizsgálatot folytat;
- b) kérelemre vagy hivatalból adatvédelmi hatósági eljárást folytat;
- c)

(1a) A Hatóság ellátja 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 (EU) 2016/679 európai parlamenti és a tanácsi rendeletben (a továbbiakban: általános adatvédelmi rendelet) a tagállami felügyeleti hatóság számára meghatározott feladatokat az ott meghatározottak szerint.

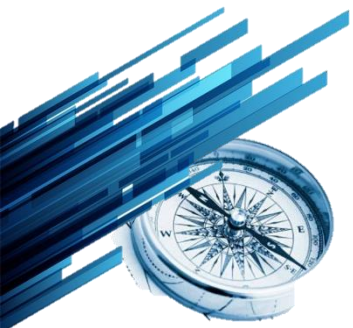


A HATÓSÁG VIZSGÁLATA

52. § (1) A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok vagy a közérdekből nyilvános adatok megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

(2) A Hatóság vizsgálata nem minősül közigazgatási hatósági eljárásnak.

(3) A Hatósághoz tett bejelentése miatt senkit sem érhet hátrány. A bejelentő kilétét a Hatóság csak akkor fedheti fel, ha ennek hiányában a vizsgálat nem lenne lefolytatható. Ha a bejelentő kéri, kilétét a Hatóság akkor sem fedheti fel, ha ennek hiányában a vizsgálat nem folytatható le. Erről a következményről a Hatóság a bejelentőt köteles tájékoztatni.



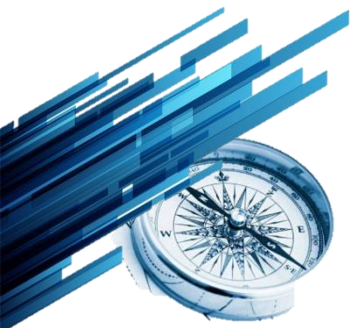
VIZSGÁLATI ELJÁRÁS

Határidő:

- Ügyintézési határidő: 2 hónap

Vizsgálati eljárás eredménye:

- Intézkedés
 - adatkezelő felszólítása
 - ajánlás felügyeleti szervnek
- Hatósági eljárás indítása
- Jelentés
- Lezárás – nem volt jogsérelem



ADATVÉDELMI HATÓSÁGI ELJÁRÁS

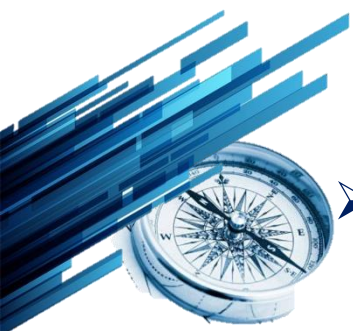
Szankciók, bírság!

Az adatvédelmi hatósági eljárás az *általános közigazgatási rendtartásról* szóló 2016. évi CL. törvény (Ákr.) hatálya alá tartozik.

Mérlegelés a szankcióknál:

- Jogsértés jellege: súlyosabb és kisebb jogsértés
- Érintettek száma: egyedi eset vagy rendszerszintű jogsértés
- Érintettek kára: fizikai, vagyoni, nem vagyoni
- A hatósággal való együttműködés
- Adatkategóriák
 - Különleges adat
 - Azonosíthatóság, azonosítás módja (közvetlen/közvetett)
 - Az adat terjesztése közvetlenül okozhat-e kárt
 - Nyilvános vagy titkosított adat
- Tudomásszerzés a jogsértésről: sajtócikk, beadvány, adatkezelő bejelentése

www.nador.hu | Telefon: +36 1 470-5000 | info@nador.hu



A HATÓSÁG ELJÁRÁSAI

Széles körű jogosítványok

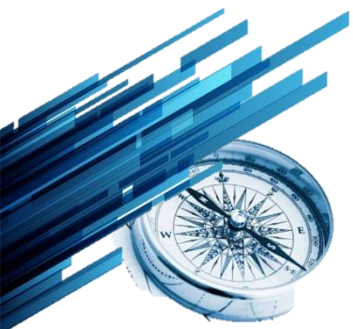
Az Adatvédelmi Hatóság (NAIH) vizsgálata során

- a vizsgált adatkezelő kezelésében levő, a vizsgált ügyel összefüggésbe hozható összes adatot megismerheti,
- az adatkezelés helyszínéül szolgáló helyiségbe beléphet, az adatkezelési műveletek végzéséhez használt eszközökhöz hozzáférhet,
- a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet.



VIZSGÁLATI ÉS HATÓSÁGI ELJÁRÁSOK ÖSSZEHASONLÍTÁSA

Vizsgálati eljárás	Hatósági eljárás
adatvédelem és információszabadság	adatvédelem
kötetlen, kevésbé formalizált	hatósági jelleg
GDPR + Infotv	GDPR + Ákr. + Infotv.
kilét felfedéséhez hozzájárulás	zárt adatkezelés
iratbetekintési jog nincs	iratbetekintési jog biztosított
felszólítás	határozat
döntés nem kikényszeríthető	kötelezés
nincs jogorvoslat	bírószági jogorvoslat
határidő: 2 hónap	határidő: 150 nap



AZ ADATVÉDELEM, MINT FEGYVER...

Igen, hatékony támadó fegyver!

Kik használják?

- nagy cégek, konkurencia legyőzésére
- sértett ügyfelek
- sértett munkavállalók

Az eszköz hatásos, mindenki követ el hibát! Olykor még a „jószándékú” bejelentő is!



KÉT TANULSÁGOS ESET

- **Adatvédelmi hatósági ellenőrzés**: ezt az előbb nem említettük, de az adatvédelmi hatósági eljárás „előszobája”. Már az Ákr. hatálya alá tartozik, tárgya a jogszabályban foglalt rendelkezések betartásának ellenőrzése. Itt a támadás egy önkormányzat ellen indult.
- **És egy vizsgálati eljárás**: tipikusan az elégedetlen (sértett) munkavállalók akciója, akik a vélt vagy valós sérelmeik okán a NAIH-hoz fordulnak, hogy marasztalja el munkáltatójukat.



A KOCSMA SZABADSÁGA

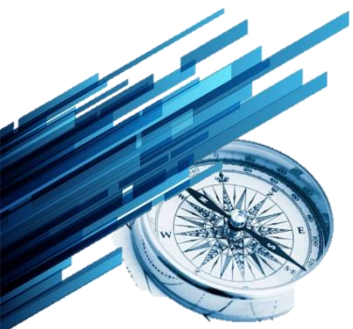
Nem, nem kocsmá, menő vendéglátó hely, kulturális programmal.

Derék vendéglátósok, akiknek mindent szabad, kötelezettségük nincsen, létezésük „nemzetgazdasági érdek”. Mentalitásuk:



- A közterületi teraszhoz nem is kell engedélyt kérni, sőt fizetni sem jó érte.
- Az önkormányzati bírságot sem szükséges befizetni, nem lehet belőle semmi baj. A bírság úgyis kevesebb, mint a közterület használati díj (legalábbis eleinte).

Végül mégiscsak benyújtották az (ingyenes) közterület használati kérelmet, melyet az Önkormányzat elutasított, a be nem fizetett bírságok miatt.



A KOCSMA TÁMADÁSA

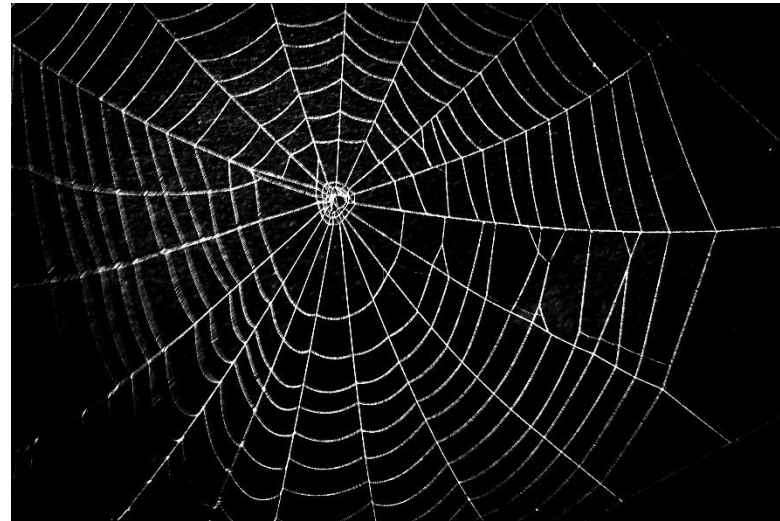
A CSAPDA

„Megfellebbezzük az elutasítást, egyúttal csőbe húzzuk az önkormányzatot!”

A szereplők:

B úr, érdekeltséggel a vendéglátó hely üzemeltetésében

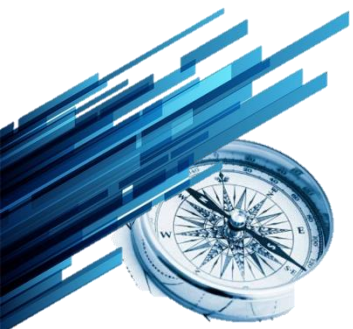
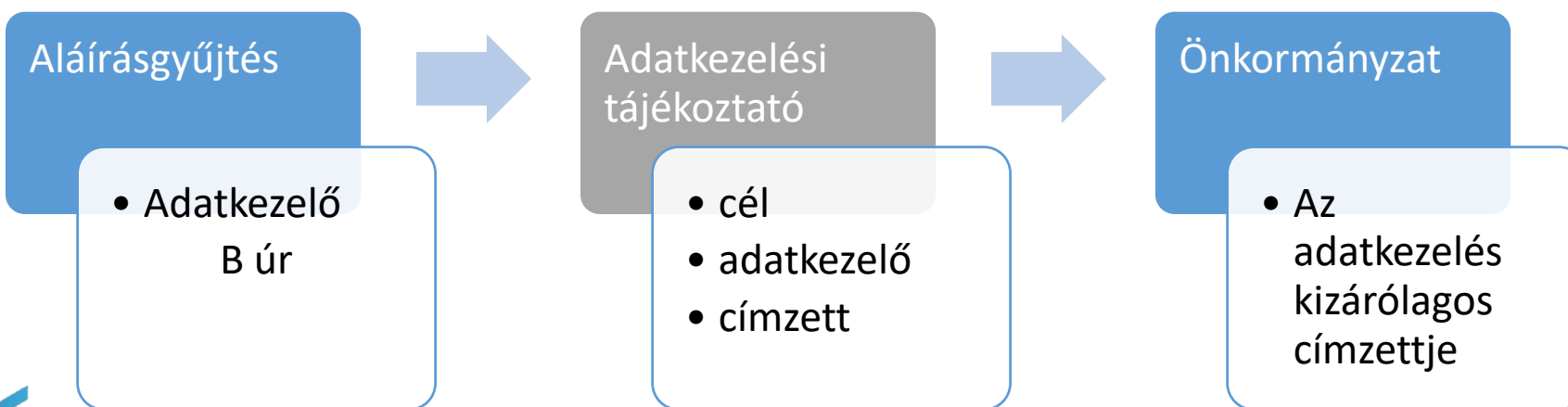
C Kft., a vendéglátó helyet üzemeltető kft.



A KOCSMA TÁMADÁSA

A CSAPDA 2

„Indítsunk petíciót a kérelem alátámasztására!”



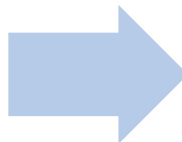
A KOCSMA TÁMADÁSA

A CSAPDA 3

Képviselőtestületi ülésre **C Kft.** benyújtja a beadványát, csatolva a petíción összegyűjtött aláíróíveket, az aláírók személyes adataival. A testületi ülések anyagait közzé kell tenni az Önkormányzat honlapján!

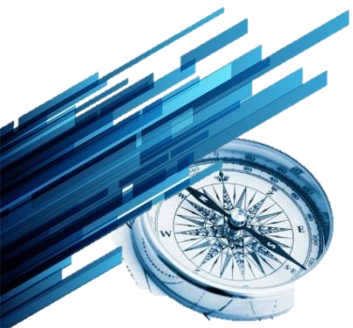
Fellebbezés
Aláírásgyűjtés

- Benyújtó
C Kft.



Kérelem és mellékletei
közzététele

- Önkormányzat
szokásos ügyrendje
szerint



A KOCSMA TÁMADÁSA

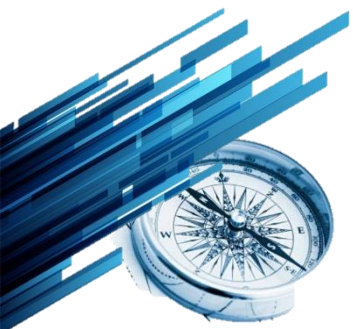
A CSAPDA BEZÁRUL!

Kedd este 10 óra:

C Kft. benyújtott kérelme, *mellékleteivel együtt* a törvényes határidőben, még kedden este 10-kor közzétételre kerül az önkormányzati portálon! A csapda bezárult! Az önkormányzat ellenőrzés nélkül, jogosulatlanul közzétette a támogatók személyes adatait!

Szerda reggel 8 óra:

A NAIH elektronikus postafiókjába megérkezik a „jószándékú” bejelentő értesítése arról, hogy milyen szörnyű adatvédelmi incidens történt az önkormányzatnál. Beindul a NAIH gépezete.



A KOCSMA TÁMADÁSA

A HATÓSÁG ELLENŐRZÉSE

A NAIH végzésben hívja fel az Önkormányzatot tájékoztatásra:



Történt-e adatvédelmi incidens?



Incidens nyilvántartást be kell nyújtani.



Mikor szerzett tudomást az incidensről?



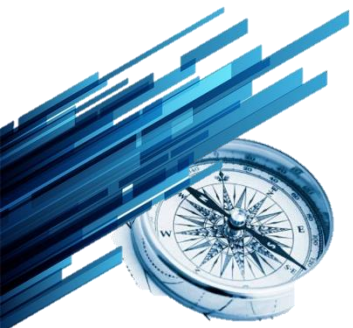
Megtett intézkedések?



Incidens kockázatai?



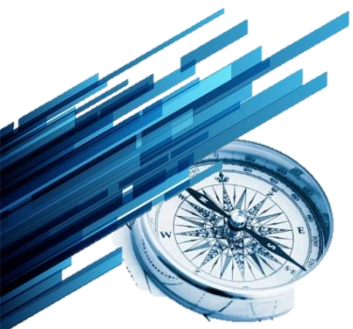
Belső eljárásrendek?



A KOCSMA TÁMADÁSA

A HATÓSÁG ELLENŐRZÉSE 2

- Az Önkormányzatot csak ezúton szerzett tudomást az incidensről. Az adatvédelmi incidens bejelentése a tudomásszerzést követően (NAIH értesítés) az előírt határidőn belül megtörtént (72 óra).
- Rendelkezésre állt az adatvédelmi incidensek nyilvántartása és a szükséges szabályzatok, köztük az incidenskezelési szabályzat.
- Az Önkormányzat értesítette az adatgyűjtést végző magánszemélyt, hogy az általa kezelt adatokkal kapcsolatban incidens történt és szíveskedjen értesíteni az érintetteket.



A KOCSMA TÁMADÁSA

A FAGYI VISSZANYAL!

A „jószándékú”, a személyes adatok védelmét olyannyira a szívéen viselő bejelentő (feltehetően **B úr**) elkövetett egy hibát: **B** nem volt jogosult átadni a petíció eredményét a **C Kft.**-nek, mert az adatkezelési tájékoztatóban a kocsmá nem volt megnevezve, mint az adatok címzettje.

Mind **B úr**, mind **C Kft.** jogosulatlanul kezelte a személyes adatokat.



A KOCSMA TÁMADÁSA

AZ ÖNKORMÁNYZAT VÁLASZA A NAIH FELÉ

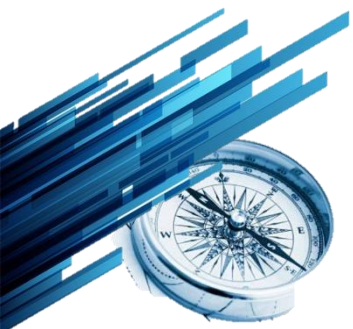
- „Felhívjuk a T. Hatóság figyelmét, hogy az Önökhöz a tárgyban tett bejelentés célja nem az incidensben érintett személyek adatainak védelme, hanem kizárólag az Önkormányzat és a Hivatal lejáratása volt. Az incidensről a Hivatalt a bejelentő nem értesítette, amely nyomán az incidens azonnal megszüntethető lett volna, ellenben a Hatóságnál egy napon belül bejelentést tett.”
- „Észrevételezzük továbbá, hogy a kérdéses aláírógyűjtő ívek adatkezelője **B** magánszemély volt, az adatkezelési tájékoztató szerint az Önkormányzat és a Hivatal volt az adatok egyedüli címzettje, ugyanakkor a Hivatalhoz az aláíróíveket a **C Kft.** nyújtotta be, aki az aláíróívek adatkezelési tájékoztatója alapján nem volt jogosult az aláíróíveket megismerni sem, nemhogy felhasználni és továbbítani.”



A KOCSMA TÁMADÁSA

HAPPY END? NINCS.

1. A NAIH ez ügyben többet nem hallatott magáról, az Önkormányzatnak nem volt további teendője, azon kívül, hogy folyamatait javítsa.
2. Nem ismert, hogy a NAIH milyen lépéseket tett a jogosulatlan adatkezelők irányában.
3. A **C Kft.** jelenleg a cégjegyzék szerint „f. a.”, azaz felszámolás alatt, s feltételezhetően nem egyenlítette ki a korábban rá kiszabott bírságokat sem.
4. A véletlen folytán, ugyanazon a helyen, ugyanazzal a profillal, ugyanazzal a tulajdonosi háttérrel egy **C2 Kft.** működik...



OKOSABB A MUNKÁLTATÓNÁL

A DOLGOZÓ MEGLECKÉZTET

A NAIH vizsgálati eljárásban fordult egy közfeladatot ellátó szervezet felé, egy meg nem nevezett bejelentő kérte a szervezet adatkezelésének kivizsgálását.

- A NAIH eljárás a szervezet „által végzett személyes adatok kezelésnek jogszerűsége tárgyában” indult.
- A Hatóság konkrét információval rendelkezett a szervezet működéséről, adott csoport tagjairól.
- Adatszolgáltatást kért név szerint megnevezett dolgozók feladat és hatásköréről, egyes jogosultságokról.
- Kérte a nevezett személyek munkakörét, beosztását.



OKOSABB A MUNKÁLTATÓNÁL

A NAIH vizsgálati eljárásában visszahivatkozik a hasonló tárgyban, egy évvel azelőtt indított vizsgálatára.

Az előző vizsgálat óta *eltelt a két hónap*, többszörösen is, amely alatt le kellett zárnia a Hatóságnak az ügyet. Most akkor miről beszélünk? Új eljárás? Új tények? A bejelentő elégedetlen volt az előző eljárás eredményével, miszerint nem volt megállapítható jogsértés a szervezet részéről?

Hogy is rendelkezik az Infotv?



OKOSABB A MUNKÁLTATÓNÁL

Az Infotv. rendelkezése a vizsgálati eljárás lezárásáról:

55. § (1) A Hatóság a vizsgálat hivatalból történő megindításától vagy a bejelentés érkezését követő naptól számított két hónapon belül

a) megállapítja, hogy (...) jogsérelem következett be, vagy annak közvetlen veszélye áll fenn, és... (intézkedést tesz...)

b) megállapítja, hogy jogsérelem nem következett be, illetve annak közvetlen veszélye nem áll fenn, és a vizsgálatot lezárja.

(2) A vizsgálat eredményéről, a vizsgálat lezárásának indokáról, esetleges intézkedéséről, illetve hatósági eljárás megindításáról a Hatóság a bejelentőt és – ha a vizsgálatban részt vett – a vizsgálat alá vont adatkezelőt, illetve adatfeldolgozót értesíti.

A Hatóság a bejelentőt bizonyára értesítette.

A vizsgálat alá vont adatkezelőt viszont nem.



OKOSABB A MUNKÁLTATÓNÁL ÉRDEKESSÉGEK A HATÓSÁG VIZSGÁLATÁBAN

A NAIH kérdései olyan konkrétumokat tartalmaztak a szervezet működéséről, dolgozóiról, melyek nem nyilvános adatok.

1. A bejelentő jogosan kezelt személyes adatokat?
2. A bejelentő hozzáfért, lemásolt olyan adatokat állításai bizonyítására, amelyek a szervezetinformatikai rendszerében kerültek tárolásra?

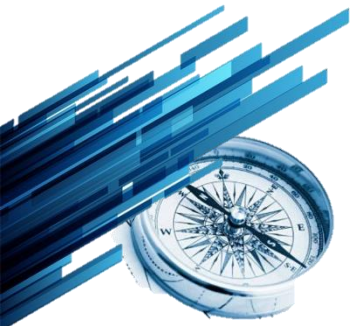


OKOSABB A MUNKÁLTATÓNÁL

KÉRDÉS A HATÓSÁG FELÉ

A szervezet vezetősége megállapította, hogy a Hatóság által megküldött kérdések alapján felmerült

1. személyes adattal való visszaélés, (Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 219. § (1) bekezdés a) pontja szerinti jogosulatlan adatkezelés, vétség)
2. Ha a becsatolt anyagban szerepelt képernyőkép, dokumentum másolat, akkor az a Btk. 422. § (1) bekezdés e) pontja szerinti jogosulatlan adatkezelés (tiltott adatszerzés, bűncselekmény!)



OKOSABB A MUNKÁLTATÓNÁL

KÉRDÉS A HATÓSÁG FELÉ

Felkértük a T. Hatóságot, hogy közöljék:

- a) milyen úton került birtokukba munkatársaink névsora, beosztása és egyéb, szolgálati jogviszonyt érintő személyes adata?
- b) Megvizsgálták-e ezen adatok megszerzésének és továbbításának jogszerűségét?
- c) Indítottak-e bármilyen eljárást a jogosulatlan adatkezelés miatt?
- d) Bocsátott-e a Hatóság rendelkezésére a bejelentő egyéb adatokat, melyek feltételezhetően a Btk. tiltott adatszerzés kategóriájába estek, s ezen adatok ügyében indult-e vizsgálat?

Amennyiben a feltételezés helytálló, abban az esetben a szervezet részéről

1. Bejelentést kell tenni a NAIH felé, adatvédelmi incidens okán.
2. Büntető feljelentést kell tenni a Btk.-ba ütköző cselekmények miatt.

Várjuk a Hatóság válaszát! (A fagyvi visszanyal?)



HA LEHET, NE LEGYÜNK ÉRINTETTEK HATÓSÁGI ELJÁRÁSOKBAN!

De ez nem mindig az adatkezelőn múlik, de meg kell tenni a megfelelő intézkedéseket!

- Szigorúan követni kell GDPR előírásait;
- Minden esetben követni kell az adatkezelés elveit:
 - jogszerűség, tisztességes eljárás és átláthatóság;
 - célhoz kötöttség;
 - adattakarékosság;
 - pontosság;
 - korlátozott tárolhatóság;
 - integritás és bizalmas jelleg;



HA LEHET, NE LEGYÜNK ÉRINTETTEK HATÓSÁGI ELJÁRÁSOKBAN!

- Az adatkezelések átláthatósága érdekében belső szabályzatokat kell kidolgozni, az érintettek számára pedig adatkezelési tájékoztatókat kell közzé tenni.
- A munkavállalók felé egyértelműen meg kell határozni az informatikai rendszerek, e-mail fiókok magáncélú használati feltételeit, az ellenőrzések módját, biztosítani kell az ellenőrzés átlátható körülményeit.
- A jogos érdeken alapuló adatkezelések során készítsünk érdekmérlegelési tesztet!
- Adatvédelmi incidens esetén AZONNAL (72 órán belül) be kell azt jelenteni a NAIH felé!



ÚTRAVALÓ

Mit tegyünk, ha szervezetünk hatósági eljárással érintett?

- legyünk együttműködők
- ne próbáljuk megváltoztatni a múltat (a Hatóság többet tud, mint gondolnánk)
- nézzük át az összes körülményt, amely arról szól, hogy teljesítettük az elvárható gondosságot
- bizonyítsuk jóhiszeműségünket (és ha lehet, akkor a másik oldal rosszhiszeműségét)



KÖSZÖNÖM A FIGYELMET!



www.nador.hu | Telefon: +36 1 470-5000 | info@nador.hu

