turizmus.com


# KÉZIKÖNYV

**A turizmus.com és**
**az EUline 9001:2001 Kft. közös kiadványa**

# MINEK NEKÜNK GDPR?

GDPR! – Ez a manapság oly sokszor hallható négybetűs szó a legkülönfélébb reakciókat váltja ki az emberből, az összerándult gyomortól a laza legyintésig.

*SZÖVEG:* ***MAKAI GÁBOR,***
*az MSZÉSZ GDPR-szakértője*

Pedig „szegény” GDPR csak egy rendelet. Az Európai Unió tavaly május óta alkalmazandó általános adatvédelmi rendelete, egy betartandó és kötelező dolog, mégse tudunk rá úgy tekinteni, mint egy számviteli vagy munkavédelmi törvényre, vagy éppen a munka törvénykönyvére. Ez olyan kis fekete bárány lett... Vajon miért? Az okát nem fogjuk most megkeresni, hiszen mindenki levonta már a maga következtetéseit, illetve vannak gondolatai a GDPR megfogalmazott követelményeivel, vagy annak előzetes és utólagos kommunikálásával kapcsolatosan.

Ha azt gondoljuk, hogy felesleges dolog, akkor csak pillantsunk át egy kicsit a másik oldalra, ahol magánszemélyként (érintettként) mi mindannyian ott állunk, és elvárjuk, hogy az általunk átadott személyes adatainkkal kapcsolatban legyenek jogaink, illetve vigyázzon rájuk, akinek odaadtuk! Ugye, ugye? Ilyen egyszerű! Csak cégként az egyik oldalon állunk, magánemberként pedig a másikon.

Tegyük most félre az egész GDPR-rendeletet, kötelező elemeivel együtt, amit az ablakba már úgyis jól láthatóan kitettünk az elmúlt egy év alatt (pl. van már „cookie” tájékoztatónk, begyűjtöttünk sok-sok hozzájárulást, illetve biztos van egy olyan tájékoztatónk és szabályzatunk, amelyben benne vannak az „adatkezelés” vagy az „adatvédelem” szavak...), így letudtuk a GDPR-t! Kipipálva! Vagy mégsem?

A GDPR csupán egy irányvonalat ad, a megvalósítás mélységét és minőségét nem hivatott pontosan meghatározni és szabályozni, ezt a szervezetre bízza, így marad nekünk a rendeletből ilyen-olyan módon leszűrhető ellenőrzési lista arról, hogy mit kell megcsinálni annak érdekében, hogy minden „rendben” legyen. Ha valaki itt megáll, az az ő döntése, csak sajnos ezt a valóságban működtetni is kell, mert az adatvédelmi incidenseket és az esetleges bejelentéseket nem a kirakatdokumentumok fogják megelőzni!

**Ha most feltenném a kérdést, hogy „Van-e értelme kiépíteni a GDPR megfelelőségi rendszert?”, akkor az egyetlen igenlő válasz így szólna: „Igen, hogy elkerüljük a büntetést!”, a legtöbb válasz pedig a „Nem!” vagy a „Semmi!” lenne.**

Ha most feltenném a kérdést, hogy „Van-e értelme kiépíteni a GDPR megfelelőségi rendszert?”, akkor az egyetlen igenlő válasz így szólna: „Igen, hogy elkerüljük a büntetést!”, a legtöbb válasz pedig a „Nem!” vagy a „Semmi!” lenne. Az én véleményem azonban az, hogy a GDPR lényegét nem a felszínen kell keresni, a helyes válasz az adatvédelem és az adatkezelés tényleges megvalósítási módszerén alapuló, napi szintű szervezeti folyamatok alkalmazása, valamint az IT megfelelő működtetése!

A következő hónapokban megjelenő cikksorozattal szeretnék egy apró kavicsot dobni a „felkészült” cégek állóvizébe, hátha a jelenleginél esetleg jobb vagy használhatóbb rendszert tud kiépíteni maga köré a szervezet, ha már egyszer ezt a „GDPR izét” kötelezővé tették. Esetleg majd lesznek olyanok is, akik meglátják benne azokat a hasznos pontokat, amelyek alapján a fenti kérdést újra feltéve a válaszok talán már ezek lesznek: „Igen, volt értelme!”

### AZ ELKÖVETKEZŐ HÓNAPOKBAN TÖBBEK KÖZÖTT EZEKRŐL LESZ SZÓ:

- adatvagyonleltár, ami nem kötelező, de nélküle nem tudunk megfelelni,
- a hozzájárulások „veszélyei” és kezelése,
- a papíralapú iratok tényleges kezelése,
- felesleges adatbázisok,
- megőrzési idők és selejtezések, törlések,
- e-mailek kezelése, dedikált e-mailek,
- e-mailes továbbítás vagy szervermegosztás szervezeten belül,
- jogosultságok, hozzáférések,
- mentések és azok visszaállítása,
- üzletmenet-folytonosság, tesztek és visszaállítás.

SZÁLLÁSHELY-VENDÉGLÁTÁS

## Minek nekünk GDPR?

# FÖLÖSLEGES HOZZÁJÁRULÁSOK

A formanyomtatványokon, a sok-sok személyes adat bekérése után általában az a félmondat szerepel, hogy „és hozzájárulok az adataim kezeléséhez…”. Minden rendben van ezzel? A GDPR-ról szóló cikksorozatunk második része következik.

SZÖVEG: ***MAKAI GÁBOR,***
*az MSZÉSZ GDPR-szakértője*

Ebben a cikkben nem arról írnék, hogy melyek a hozzájárulás feltételei, ezt a GDPR 7. cikke bemutatja nekünk. A kérdés, amit körbejárunk, hogy a hozzájárulást, mint adatkezelési jogalapot egyáltalán mikor, és vajon az összes megadott személyes adatra érdemes-e alkalmazni?
A GDPR rendelet 6. cikke hatféle joglappal indított útnak bennünket: hozzájárulás, szerződés teljesítése, jogszabályi megfelelés, adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése, az érintett érdekeinek védelme, közérdekű feladat végrehajtása. Ezekből lehet kiválasztani azt, amelyik a legmegfelelőbb az adott adatkezelési célra. A két utolsó jogalapot nem nagyon fogom emlegetni, mert ebben a szektorban nem igazán relevánsak.
Első nekifutásra a hozzájárulásos jogalap tűnik a legegyszerűbbnek és legkezelhetőbbnek, hiszen egy hozzájárulást – a GDPR 7. cikkének figyelembevételével és betartása mellett – igazán egyszerű bekérni. Az érintett úgyis azonnal aláírja, bepipálja, megadja, mert őt a jogalapok nem igazán érdeklik, ő csak szeretné megkapni a szolgáltatását, termékét. Ráadásul úgy tűnik, hogy ez az eljárás működőképes, minden gond le van vele tudva, nem is kell más jogalapon gondolkodni, hiszen az érintett hozzájárult…
Tényleg ilyen egyszerű lenne? Valóban jó dolog, hogy adott esetben minden személyes adatot egy kalap alatt, egy hozzájárulási jogalappal kezelünk az adott adatkezelési cél megvalósítása érdekében? Hogyan tudjuk eldönteni, hogy jól csináljuk-e? Egyszerűen!
Csak vizsgáljuk meg, mi történik, ha éppen úgy gondolja az érintett, hogy nem járul hozzá az adatkezeléshez, vagy éppen visszavonja a hozzájárulást. Mert ez megtörténhet, ez ennek a jogalapnak a sajátossága! Akkor jöhetnek a magunknak feltett kérdések. Tudunk-e bármely személyes adat hiányában jogszabálynak megfelelni, szerződést teljesíteni, vagy esetlegesen életszerűen működtetni a szolgáltatásunkat?
Ha nem, akkor másik jogalapo(ka)t kell választani az adott személyes adatnak.
A többes szám nem véletlen, hiszen egy adatkezelési célon belül személyes adatonként lehet több jogalapot is alkalmazni. Gondoljunk csak egy „sima” szállodai bejelentkezésre, a bejelentőlapon felvett adatokra. Van benne jogszabályi megfelelés, szerződésteljesítés, talán jogos érdek, illetve, ha van rajta pl. hírlevélre való feliratkozás, akkor hozzájárulás is.
Én személy szerint – anélkül, hogy rangsort állítanék – a vonatkozó jogszabályi kötelezettség feltérképezésével kezdeném, ezt követően a szerződés teljesítéséhez való szükségességet nézném meg, majd a jogos érdekeket vizsgálnám. Megjegyzem, vannak egyértelmű hozzájárulásos jogalapon működő adatkezelések, ahol nincs is lehetőség más választásra!
Ha sikerült mindent megfelelő jogalapra tenni, akkor nézzük meg, hogy érdemes-e azt még „bebiztosítani” egy hozzájárulással? Úgy gondolom, hogy fölösleges, de ami még rosszabb, becsapjuk vele az érintettet is! Csak egyszerűen bele kell gondolni, hogy mi történik akkor, ha visszavonja a hozzájárulását, mert tudja, hogy megteheti. Akkor kezdünk el mesélni neki arról, hogy nem tudjuk megszüntetni az adatkezelést, mert az adatok szükségesek a jogi kötelezettség teljesítéséhez?
Akkor minek kell fölösleges köröket futni? Mert bár a megfelelő jogalapok pontos meghatározása többletmunkával jár, a hosszútávon jelentkező előny megkérdőjelezhetetlen. Ezért ne tévesszük meg az ügyfelet és magunkat. Ahol valóban kell, ott kérjük be a hozzájárulást, a többiről pedig megfelelően tájékoztassuk az érintettet az adatkezelési tájékoztatónkban!

*Kérdéseiket az alábbi e-mail címen tehetik fel a szakértőnek: makai@euline.hu*

# ADATVAGYONLELTÁR – A SZÜKSÉGES ROSSZ

Az adatvagyonleltár összeállítása a GDPR-felkészülés talán legnehezebb része, amire sokan úgy tekintenek, hogy elhagyható. Vagy mégsem? Az adatvédelmi rendeletről szóló cikksorozatunk harmadik részéből kiderül.

SZÖVEG: ***MAKAI GÁBOR,***
*az MSZÉSZ GDPR-szakértője*

**A GDPR-rendeletben** nagyítóval sem találjuk meg azt a varázsszót, hogy „adatvagyonleltár". Így joggal gondolhatjuk, hogy nincs is rá semmi szükség, nemhogy még kötelezően el is kelljen készíteni.
A gyakorlatban mégsem lehet megúszni az adatvagyonleltár összeállítását, mégpedig a felkészülés egyik első lépéseként. Ennek hiányában ugyanis nehéz kiépíteni a megfelelő GDPR-rendszert, megfelelni bizonyos rendelkezéseknek, illetve, ami még fontosabb, átlátni az adatkezeléseinket, elkészíteni az adatkezelési eljárásrendet és működtetni a bevezetett rendszert.
Az összes nálunk kezelt adat valamilyen értéket képvisel, a vagyonunk része. Akkor miért is ne vennénk leltárba, mint az összes többi értékes és kevésbé értékes materiális vagyonelemünket?
Amikor egy új eszköz, berendezés kerül a szervezethez, azonnal leltárba vesszük, címkézzük, nyilvántartást vezetünk róla, amelyben összegyűjtjük a számunkra fontos információkat.
Pont ugyanezt kell tenni az adatvagyonelemekkel is. A „Bejelentőlap" ebben a tekintetben nem sokban különbözik egy forgószéktől, a „Vacsoralista" egy állólámpától, az „Online űrlap" a falitükörtől, a „Munkatársi nyilvántartás táblázata" az íróasztaltól. Amint látjuk, az adatvagyon elemei mindenhol jelen vannak. A Front Desken, a munkaügyön, a pincéreknél, a garázsmesternél, az aláírt slipen...
Sajnos a teljes, pontos, naprakész adatvagyonleltár elkészítése nem kevés munkával járó feladat, és az sem túl jó hír, hogy egyik GDPR-tanácsadó sem tudja helyettünk jól elkészíteni, hacsak be nem költözik hozzánk egy-két hónapra. Ő csak támogatni tudja a munkát, vezetni a kezeket.

## ADATKEZELÉSI CÉLTERÜLETEK ÉS ÉRINTETTEK

Miután mindenkinek elvettük a kedvét az adatvagyonleltár elkészítésétől, lássunk is hozzá!

**Első lépésként** határozzuk meg, hogy milyen adatkezelési célterületeink (folyamataink) vannak. Ezt már célszerű az érintettek csoportjai (munkavállalók, szállóvendégek, online felhasználók stb.) szerint bontani.
Gondolatébresztőnek néhány adatkezelési célterület, ha az érintett a szállóvendég: érintettek kamerás megfigyelésével kapcsolatos adatkezelés; hírlevél-szolgáltatással és egyéb marketingtevékenységgel kapcsolatos adatkezelés; elégedettségméréssel kapcsolatos adatkezelés; klubtagsággal, törzsvásárlókkal kapcsolatos adatkezelés. Szállásfoglalással kapcsolatos adatkezelés telefonon, személyesen;panaszkezelés.
Az adatkezelési célterületek meghatározása és vele az adatvagyon elkészítése a legjobb alapja a tájékoztatók és az eljárásrendek elkészítéséhez. Az érintett csoportonkénti szétválasztás pedig megkönnyíti az egymástól független tájékoztatók elkészítését, és így később átláthatóbb is lesz a rendszer.

**A második lépésben** keressük meg azokat a munkatársainkat, akik saját munkafolyamataik során papíralapú és elektronikus dokumentumokat, formanyomtatványokat, adatbázisokat (egyszóval adatvagyont) kezelnek, és kezdjük el ezeket összeírni!
A GDPR 30. cikke szerinti, pontokba szedett nyilvántartási kötelezettséget feltétlenül teljesítsük! Továbbá én úgy gondolom, hogy mélyebbre is lehet és kell is ásni ahhoz, hogy egy jól működő és használható adatkezelési rendszert tudjunk kiépíteni. Ez az adatvagyonhalmaz kell ahhoz, hogy egy korrekt tájékoztatót meg tudjunk írni, vagy éppenséggel az adatkezelési eljárásrendünk kialakításakor tisztában legyünk azzal, hogy pontosan kinek, milyen személyes adatait, hol, hogyan gyűjtjük, azokat hol tároljuk, mikor töröljük, kik láthatják...
A leltárt elkészíthetjük papíralapon (de nem javaslom), Excel-táblában, illetve léteznek már célprogramok, amelyek nagyban megkönnyítik ennek a nagy információhalmaznak a jövőbeli kezelését, illetve hatékonyan támogatják a kialakított adatkezelési rendszerünket.

*Kérdéseiket az alábbi e-mail-címen tehetik fel a szakértőnek: makai@euline.hu*

# JOGOSULTSÁGOK KEZELÉSE – TUDATOSAN

A lakásunkat is zárjuk, és pontosan tudjuk, kit engedünk be oda. A gyerekek sem nézhetnek akármit a tévében, és apa gépét sem használhatja bárki a hozzáférések és jogosultságok jól átgondolt otthoni rendszerében. A szállodánkban se legyen ez másképp!

SZÖVEG: ***MAKAI GÁBOR,***
*az MSZÉSZ GDPR-szakértője*

**Az adatvédelmi rendeletről** szóló cikksorozatunk negyedik részének témája nem ismeretlen azok előtt, akik szállodát működtetnek, hiszen jogosultságokat minden munkaterületen ki kell osztani: a szállodai szoftver működtetéséhez, a számítógépek, e-mail címek használatához, a szobákba, a szerverterembe, az irattárba történő belépéshez, a hálózati meghajtón tárolt adatok kezeléséhez, és még sorolhatnánk.
A kérdés csak az, hogy ezeket a jogosultságokat szabályozott keretek között, tudatosan kezeljük-e, vagy csak a régi, jól bevált szokásrendszerek működnek? A teljes jogosultsági rendszer kiépítése a sok apró részlet miatt hónapokba is beletelhet, és legalább ugyanennyi időt emészthet fel a működtetésébe történő „belerázódás". Ezt sajnos nem lehet megúszni, hiszen az információbiztonság alapkövetelményét, miszerint az információ csak az arra felhatalmazottak számára legyen elérhető, egyebek mellett egy alaposan átgondolt jogosultsági rendszer létrehozásával és működtetésével lehet megvalósítani.
A téma komolyságát jelzi, hogy Portugália első GDPR-ral kapcsolatos ítéletét többek között épp a jogosultsági rendszer hiányosságai miatt hozták meg az év elején (a Barreiro Montijo Központi Kórházat 400 ezer euróra bírságolták az ügyben).

## AZ ELRENDELÉSTŐL A VISSZACSATOLÁSIG

Hogyan is álljunk neki? Az első lépés, hogy felkutatjuk, kinek milyen adatokat lehet, illetve kell kezelnie a munkafo-

lyamatok során. Az előző cikkemen felbuzdulva valószínűleg már mindenki elkészítette az adatvagyonleltárt, ezt nagyszerűen felhasználhatjuk ebben a munkafázisban.
Innentől jön a megvalósítás, amely a szervezet vérmérsékletének megfelelő mélységű és részletességű, működtethető és működő rendszer kidolgozását, bevezetését és fenntartható működtetését jelenti.
Most csak néhány gondolatébresztő kérdést teszek fel, amelyek jó tükörként szolgálhatnak arra, hogy az olvasók kiderítsék, rendelkeznek-e jól működő, tudatosan kiépített jogosultsági rendszerrel.
Pontosan meghatározták-e és dokumentálták-e a szervezetnél az egyes munkakörökhöz (csoportokhoz, személyekhez) tartozó jogokat?
Tudják-e, hogy ki(k)nek a felelőssége, feladata a hozzáférési módozatok (beállítás, módosítás, törlés) elrendelése és tényleges elvégzése?
Van-e kidolgozott módszerük a fentiek menetére?
Létezik-e dokumentáció az elrendeléstől a végrehajtáson át a visszacsatolásig annak érdekében, hogy a folyamat nyomon követhető és visszaellenőrizhető legyen?
Átvizsgálták-e már, hogy az egyes munkatársaknak valóban feltétlenül szükségük van-e az összes jelenlegi hozzáférésre a feladatuk elvégzéséhez?
Lekorlátozták-e a hozzáféréseket a szükséges minimumra?
Az általános jogokon túlmenően mekkora figyelmet fordítanak a különleges, egyedi jogokra?
Vezetnek-e naprakész nyilvántartást arról, hogy kinek mihez van hozzáférése, milyen jogai vannak?
Rendszeresen ellenőrzik-e a kiadott jogokat, hogy azok még mindig megfelelnek-e a szervezeti elvárásoknak?
Tudják-e, hogyan kell azonnal reagálni egy esetleges teljes jogmegvonás (pl. rendkívüli fegyelmi eljárás) esetén?
Vannak-e olyan rendszerek, amelyek ellenőrzik a jogosultság szerinti hozzáféréseket?

## A LEGFONTOSABB TERÜLETEK

Végül pár példa arra, hogy milyen területeket érdemes most azonnal alapból átvizsgálni és a rendszer részévé tenni:

- Területekre történő, illetve a biztonsági és egyéb zónákba történő belépés;
- Adatbázisokhoz, programokhoz történő hozzáférések;
- Helyi hozzáférések (szerverek, munkaállomások, egyéb eszközök hozzáférései);
- Megosztott erőforrásokhoz való hozzáférések (mappák, nyomtatók);
- VPN, Teamviewer, távoli elérések;
- E-mailek, csoport e-mailek, webes felületek jogosultságai (pl. NAV ügyfélkapu);
- ADMIN jogok egyes kiadott eszközökön (laptop, telefon);
- A szállodán kívülre kivitt adathordozó eszközök (laptop, telefon, HDD).

*Kérdéseiket az alábbi e-mail-címen tehetik fel a szakértőnek: makai@euline.hu*

# turizmus kft.

innovatív marketingkommunikáció

TOP 50

BUSINESS TRAVELLER HUNGARY

BUSINESS EXCELLENCE

VENDÉGLÁTÁS MAGAZIN

TURIZMUS.COM BULLETIN

TURIZMUS.COM

TURIZMUS.COM MAGAZIN

BUSINESSTRAVELLER.HU

TURIZMUS.COM

OFFICIAL BUDAPEST CITY MAP

VENDÉGLÁTÁS AKADÉMIA

RÁDIÓ

VENDEGLATASMAGAZIN.HU

BUDAPEST MICE GUIDE

MICE

PR IN HUNGARY

BUSINESS DAY

TURIZMUS ÉVADNYITÓ GÁLA

/turizmuscom

# Üzletmenet-folytonosság és GDPR

**A GDPR-ról szóló cikksorozatunk 5. részéhez érve lassan elmondhatjuk, hogy rendszerünk kezd tudatos információbiztonsági mederben működni. De sajnos messze még az alagút vége. A következő lépés az üzletmenet-folytonossági rendszer kidolgozása.** **MAKAI GÁBOR, az MSZÉSZ GDPR-szakértője**

Mai témánkhoz a GDPR 32. cikke kapcsolódik, amely kimondja, hogy az adatkezelőnek és az adatfeldolgozónak megfelelő technikai és szervezési intézkedéseket kell végrehajtania annak érdekében, hogy garantálja a kockázat mértékének megfelelő szintű adatbiztonságot. Részben ehhez nyújthat segítséget, ha elkészítjük a szálloda üzletmenet-folytonossági rendszerét. Itt azonban sokkal többről van szó, mint a GDPR-nak való megfelelésről.

Azt gondolom, senkit nem kell arról meggyőzni, mennyire fontos egy szállodában a működés folytonosságának biztosítása. A folyamatok akadozása, leállása az esetek többségében nem vezet adatvédelmi incidenshez, „csupán" a vendég elégedetlenségéhez, aminek azonban soha nincs jó vége.

## IT-üzemeltetési dokumentum és szolgáltatáslista

Most csupán egy rávezető gyakorlatot szeretnék bemutatni, amelynek alapján mindenki elkészítheti a saját üzletmenet-folytonossági rendszerét a neki megfelelő mélységben és területeken.

Minden olyan esetet vegyünk figyelembe, amikor az akadozás, leállás hatással van a működésünkre és a megítélésünkre. Ilyen eset lehet például a „vendégwifi" leállása, vagy ha a biciklikölcsönzőben lefagyott a kis PC, és nem tudjuk kinyomtatni az átvételi bizonylatot.

Első körben mérjük fel, hogyan is működik az informatikai rendszerünk, milyen módszerek (új eszköz beszerzése, tartalékeszköz beállítása, javítás stb.) léteznek a működés helyreállítására, illetve ezek mennyi időt vesznek igénybe. Egyszóval egy komplett IT-üzemeltetési dokumentumot kérjünk az érintett szakembereinktől. Mi eközben írjuk össze a folyamatainkat, szolgáltatásainkat, amelyek zökkenőmentes működését mindenképpen fontosnak érezzük, amelyeknek a kiesése „gondot okozhat".

Az IT-üzemeltetési dokumentum és az általunk összeállított szolgáltatási lista alapján határozzuk meg a köztük lévő kapcsolatokat, azaz nézzük meg folyamatonként, szolgáltatásonként, hogy mi kell a működéséhez! A „vendégwifihez" például kell áram, működő internetszolgáltatás, wifi router stb. A biciklikiadáshoz egy működő PC, jogtiszta szoftver a

gépen, nyomtató, papír stb. Bármely elem meghibásodása, hiánya gátolja a folyamat megfelelő működését. Ezen módszer segítségével tudni fogjuk, hogy mely komponenseknél kell keresni a hibát, ha nem működik egy folyamat, valamint milyen szolgáltatásokat, folyamatokat veszélyeztet, ha egy eszköz leállt.

## AKCIÓTERVEK

Az előző példák elég egyszerűek, említsünk meg néhány komolyabbat is: a vendég bejelentkeztetése a szállodai szoftverbe, online szobafoglalás, árajánlatadás e-mailben, bérszámfejtő szoftver, kártyaíró szoftver az ajtónyitáshoz stb. Ezek leállásától már jobban félünk, ugye? Persze egyiktől jobban, a másiktól kevésbé. De melyik az a tényező, amit még nem vizsgáltunk? Az időkiesés! Csak gondoljuk át, mennyi időkiesést „bírunk ki", ha ezek a rendszerek nem működnek! Más-más kiesési idő más-más hatásszintű problémát generál, aminek megfelelően alternatív akcióterveket érdemes készíteni.

Például: három percig nem megy a szállodai szoftver – ez nem probléma, nincs szükség külön intézkedésre. Húsz percig nem megy – leültetjük a vendéget, és meghívjuk egy kávéra. Két órán át nem megy – a vendég ingyen szobát kap...

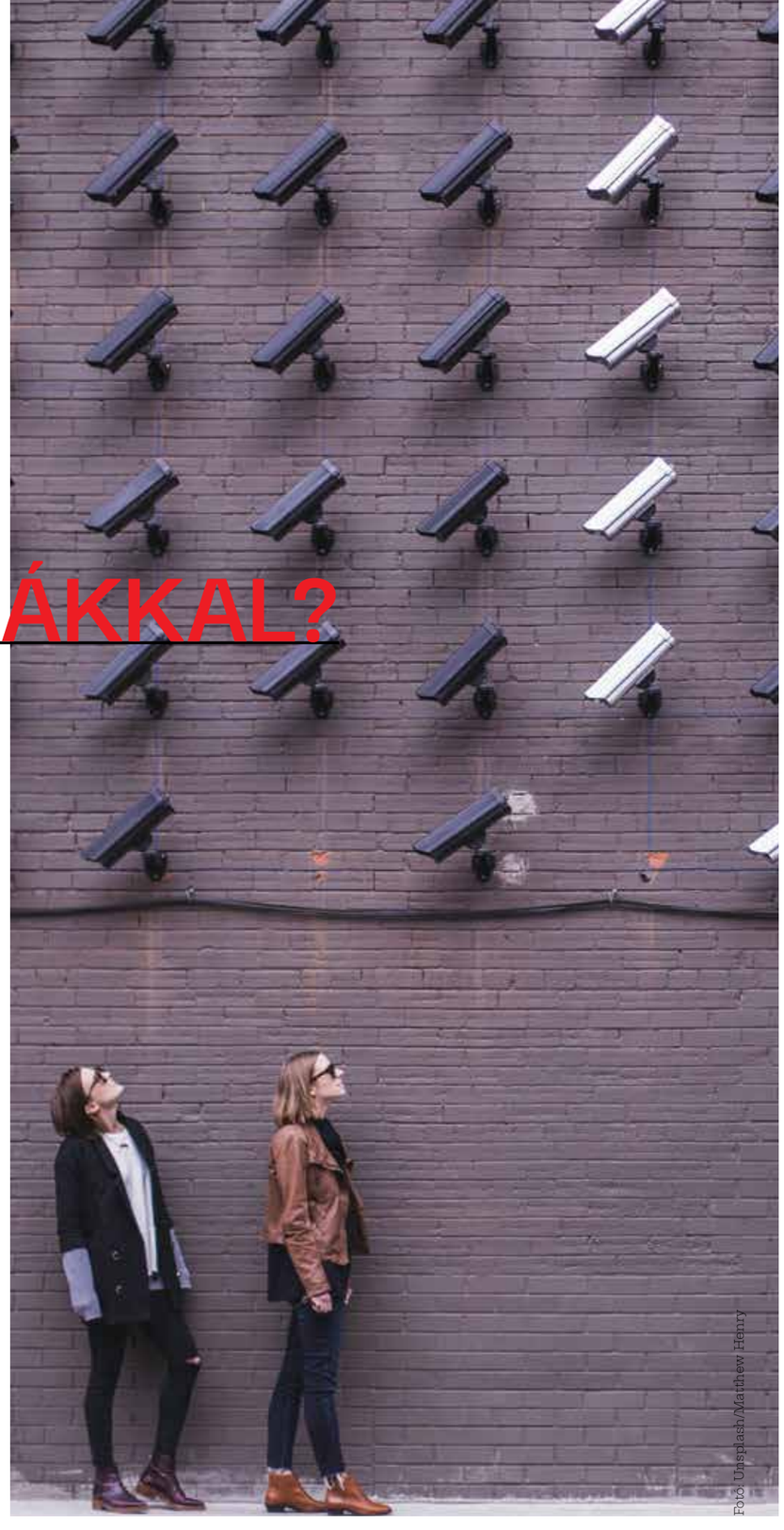
Az akciótervnek köszönhetően a probléma eközben a háttérben rendeződik, mivel már tudjuk, hogy mi okozhatta, hogy a recepciós nem tudja bejelentkeztetni a vendéget. És ez itt a lényeg! Ezért kell ismernünk minden egyes folyamat komponenseit, ezért kell ismerni ezen komponensek hibáinak helyreállítási módjait. Sajnos számos helyen találkoztunk olyan reagálásokkal a témában, mint hogy „ha baj lesz, akkor majd kitalálunk valamit", vagy „az informatikusok úgyis tudják, mit kell tenni..."

Én azt mondom, ne akkor rohangáljunk, ha már bekövetkezett a baj, hanem legyenek pontos terveink arra vonatkozóan, hogy mit kell csinálni, kit kell értesíteni, milyen alternatív megoldási módok léteznek, hogyan állítható helyre a folyamat a legrövidebb úton. És a megoldásokat célszerű le is tesztelni. Tehát érdemes ahhoz hasonlóan eljárni, ahogy egy esetleges tűzeset bekövetkezésére is felkészülünk. Szerencsére most még nincs tűz, nem ég semmi, bőven van idő és lehetőség felkészülni!

**A GDPR-ról szóló cikksorozatunk 6. részében az egyik legkönnyebben ellenőrizhető és itthon egyre több büntetéssel sújtott, rendelet által szabályozott területtel, a kamerás megfigyeléssel foglalkozunk.**

**MAKAI GÁBOR,**
**AZ MSZÉSZ GDPR-SZAKÉRTŐJE**

# Hogy állunk A KAMERÁKKAL?



Fotó: Unsplash/Matthew Henry

Azzal ma már mindenki tisztában van, hogy a biztonsági kamerák működtetése személyes adatok kezelésével jár, így ilyen tevékenységet csak a mindenkori adatvédelmi szabályok és a GDPR-rendelet egyéb vonatkozó követelményeinek betartásával lehet végezni.
Most csak pár gyakorlati dolgot emelnék ki, amire érdemes figyelnünk.

## JOGOS ÉRDEK

„Lazításként" kaptunk egy új jogalapot a kamerás megfigyelés kezelésére, ez a jogos érdek. Erre ezért volt szükség, mert a hozzájárulás, mint adatkezelési jogalap alkalmazása a gyakorlatban nem volt kivitelezhető, ennek ugyanis az a sajátossága, hogy azt az érintett bármikor visszavonhatja, aminek következtében törölnünk kellene a személyes adatot (vagyis a kép-, illetve hangfelvételt).
E jogalap alkalmazása azonban adminisztrációs kötelezettséggel is jár, hiszen a jogi megfeleléshez el kell végezni az ún. érdekmérlegelési tesztet, amiről tájékoztatni kell az érintetteket. Ezért következő feladatunk a teszt elkészítése és a tájékoztatók átírása.

## TÁJÉKOZTATÓK

A tájékoztatókat a bejáratnál kell elhelyezni, jól látható módon. Sajnos nem lesz elegendő egy egyszerű piktogram, mivel a megfigyelés ténye mellett egyéb információkat is az érintett tudomására kell hozni.
Sokan nem szívesen csúfítják el a gyönyörű bejárati üvegajtót egy A4-es méretű tájékoztatóval. Megpróbálhatunk terveztetni egy mutatósabb tájékoztatót, vagy egy másik megoldás, hogy a részletes dokumentumot a recepciónál helyezzük el, a bejáratnál pedig csak ennek a helyére hívjuk fel a figyelmet. A végeredmény sajnos sem így, sem úgy nem lesz túl szép...
Ha már gyártjuk a dokumentumokat, akkor ne felejtsük el, hogy kötelező minden kamerát külön megemlíteni, látószöggel vagy a megfigyelt terület megnevezésével, céljával.

## KÖZTERÜLET

Kevés olyan szállodában jártam, ahol a kamerák ne láttak volna valamennyi részletet a közterületből. Ez az egyik legkönnyebben támadható felület, és szerintem mindenki érzi, hogy nem 100%-ig teljesíti az ilyen irányú kötelezettségeit.
Természetesen a hatóságoknak és egyes magánszemélyeknek óriási segítség volt eddig, hogy egyes kameráink „véletlenül" látták a közterületet, és segítettek néhány ügy megoldásában, de sajnos meg kell felelnünk a követelményeknek, úgyhogy itt a következő feladat, irány a kameraszoba, vizsgáljuk át a kameraképeket, és ahol szükséges, ott jöhet a maszkolás, a kamerák elforgatása vagy a látószögek csökkentése.

## HOZZÁFÉRÉS

Végül jöjjön egy izgalmas módosítás: a jogalkotó törölte a videofelvételek felhasználásával kapcsolatos korlátozásokat, így a jövőben nem szükséges jogát vagy jogos érdekét igazolnia annak, aki a rögzített felvételbe betekintést kér, vagy arról másolatot igényel. A kamerafelvételeket pedig már nem csak bírósági és hatósági eljárás során lehet felhasználni.
Csak bízhatunk benne, hogy az új szabály kihasználása nem lesz olimpiai szám az elégedetlen vendégek körében.
Ne nagyon keressünk indokokat arra, hogy miért nem adjuk ki a felvételeket, mert sorra jönnek ki azok a NAIH-határozatok, amelyek alapján esélyünk sincs.
Ne próbálkozzunk azzal sem, hogy azért nem adjuk ki a képet, mert mások is szerepelnek rajta, ugyanis már erre is van kész válasz: „A harmadik személyek jogainak és szabadságainak védelme nem szolgálhat általánosságban indokul a felvételek kiadásának megtagadására, ehelyett az adatkezelőnek meg kell tenni a lehetséges technikai intézkedéseket (pl. a felvétel egyes részeinek kivágása, vagy az egyéb a felvételek tartózkodó személyek kihomályosítása) annak érdekében, hogy az érintett hozzáférési jogát biztosítani tudja".

Jaj de jó, gyűlnek a feladatok! Képezzünk ki egy-két munkatársat (a hozzáférésre jogosultak közül), akik értenek a felvételek kiírásához, szerezzünk be valami szerkesztőprogramot, aminek a segítségével különböző trükköket tudunk végrehajtani annak érdekében, hogy meg ne sértsük egy harmadik fél személyiségi jogait, ha kiadjuk a felvételt az általunk vásárolt adathordozón! Cinikusnak tűnhetek, de sajnos ez most komoly...
Nem visszatartó erő, de segítség lehet, ha már megtalált minket az érintett az ez irányú kérésével, hogy kérhetünk tőle a beazonosításhoz szükséges információkat, például hogy jelölje meg azt az időintervallumot (esettől függően ésszerű mértékben), amikor a kamera látószögében tartózkodott.
Akkor hát kezdődjön a munka, elő a már meglévő kamerás dokumentumokkal, jöjjön a módosítás, átírás és újrakiadás, nézzék át a kamerarendszert, hogy valóban mindenhol szükség van-e kamerára ott, ahol most fel van szerelve (ez egyébként az adattakarékosság és az érdekmérlegelési teszt része is), valamint a gyakorlatban is készüljenek fel arra, hogy esetleg felvételt kell majd kiadniuk, mert, mint minden adatkezelési témában, itt is az érintett az úr!

**Emlékszem, annak idején sok-sok fejtágításon vettem részt, ahol a tanácsadóknak és a cégeknek is azt javasolták, hogy a „kirakat“ legyen rendben minél előbb. Hiszen ezt a legegyszerűbb megcsinálni, és ha ez megvan, akkor azonnal úgy tűnik, mintha „GDPR-kompatibilis“ lenne a szervezet.**

**MAKAI GÁBOR, AZ MSZÉSZ GDPR-SZAKÉRTŐJE**


Fotó: Bigstock

# A KIRAKAT,
## ÉS AMI MÖGÖTTE VAN

Cikksorozatunk eddigi részeiben nem a kirakatrendezés, hanem rögtön a GDPR belső, valós működtetésének rejtelmeibe kalauzoltuk Önöket. Ennek két oka volt. Egyrészt úgy gondolom, a „GDPR-kompatibilis” életnek a tudatos és megfelelő működtetés a kulcsa, ezt egyébként a külföldi és magyar bejelentések és büntetések is alátámasztják.

A másik ok, hogy a kirakatot sok vállalkozó kedvű cégvezető és tanácsadó pillanatok alatt meg tudja csinálni az interneten elérhető anyagok segítségével. Ezzel nincs is semmi baj, hiszen rengeteg cégnek már ez is eléggé felemésztette a humán kapacitásait és az anyagi forrásait. Ám, ha legalább eddig eljutottunk, akkor ne álljunk meg ezen a szinten, hanem próbáljuk meg átvizsgálni, akár a cikksorozat segítségével az eddig kialakított rendszerünket, mert a legfontosabb cél a tényleges, tudatos működtetés.

Ehhez azonban idő kell, két-három évbe is beletelik, mire egy szervezet beletanul a GDPR rendszerébe, és ennek működtetése rutinszerűvé válik (a GDPR hatályba lépése és a türelmi idő lejárta között eltelt két év erre épp elegendő lett volna…).

### MÁR A WEBOLDALAKON SOK A HIBA

Személyes tapasztalataim alapján azonban gyakran a „kirakattal” sincs minden rendben. Gondoltam, készítek ezekből egy csokrot. Az elmúlt időszakban, civilként lépten-nyomon belebotlottam olyan, kirívó problémákba, amelyeket minimális erőfeszítéssel és egy kis odafigyeléssel meg lehetne oldani.

Nézzük először az internetes oldalakat:

- Lassan 2020-at írunk, és még mindig léteznek nem biztonságos weboldalak rengeteg szálloda esetében is, olyanok, amelyeken online foglalásra és kártyaadatok megadására is van lehetőség. Érdemes megnyitni az oldalunkat, és a böngésző ablakban rápillantani a „www” előtt álló „http” betűsorra. Ha ennek végéről hiányzik az „s” betű („secure”), azaz nem úgy kezdődik a cím, hogy https://www., akkor bizony érdemes gyors megoldást keresni.
- Vizsgáljuk át, hogy egy adott linkre történő kattintáskor valóban a hivatkozott dokumentumok jönnek-e elő, tényleg a „Tájékoztató” vagy a „Szabályzat” ugrik-e fel?
- A tájékoztatók tartalmát itt nem részletezem, ott van rá a GDPR megfelelő cikke, amit viszont általánosságban kijelenthetünk, hogy a 4-5 mondatos tájékoztatások nem feltétlenül elégítik azt ki, pláne, ha az adatkezelési célokat sem látjuk világosan.
- Az online felülettel kapcsolatosan van adatkezelés bőven, ezeket egyeztessük a szerver üzemeltetőjével, a weblap-üzemeltetővel, a marketingesekkel, majd az iránymutatásaik alapján készítsük el a megfelelő tájékoztatót.
- Cookie... Az ezzel kapcsolatos tájékoztatásra, de főleg ennek kezelésére kiváló IT-megoldások léteznek már. Nem árt, ha a netező azonnal ki tudja kapcsolni az eltérő szintű cookie-kat az oldalon, mert bizony vannak a működéshez elengedhetetlen cookie-k, és vannak olyanok, amelyek nem azok. Nem vehetjük őket egy kalap alá!
- Szerencsére a hírleveles checkboxok már többnyire külön vannak választva az egyéb „ikszelgetős” dobozoktól, de nézzük meg mellette a szöveget, elég egyértelmű-e, hogy mit is jelöltetünk be az érintettel?

### TÁJÉKOZTATÓK – NÉHA VAN, DE INKÁBB NINCS

De haladjunk tovább a recepció felé. Privát utazásaim során (is) belenézegetek az adott szálláshelyek tájékoztatóiba, csak azért, hogy egy-két jó ötletet merítsek, bár általában inkább a hiányosságokat veszem észre (akinek nem inge…):

- Egy panzióban elkértem a tájékoztatót, mire az a válasz érkezett, hogy „Van olyan, fent van a neten...” Sajnos olyan gép nem állt rendelkezésre, ahol el lehetett volna érni, ebben az esetben talán egyszerűbb lett volna egy nyomtatott változatot odaadni.
- Egy kisebb szállodában már volt nyomtatott tájékoztató, meg is kaptam, de a vendégről (azaz rólam) mindösszesen négy sort találtam, mely a „bejelentkezéssel kapcsolatos” adatkezelésről szólt, az egész dokumentum a munkavállalók adatkezelését taglalta.
- Több helyen a „Szabályzatot” kaptam meg, ami remek, hogy van, de abban egy szó sem volt a tájékoztatásról...

Helyezzünk el a recepciósnál nyomtatott példányokat a meglévő tájékoztatóinkból, szabályzatainkból, de tudjuk azt is – a recepción dolgozó kollégákkal együtt –, hogy mik ezek, mi a tartalmuk.

### ELLENŐRIZETLEN ADATOK

Miért nem ellenőrzi senki a recepción, hogy pontosan hogy hívnak engem, a bejelentkező vendéget, vagy, hogy pontos-e az általam beírt személyiigazolvány-szám? Így hogyan garantált a pontos adatrögzítés?

Számomra furcsa, hogy a következő mondatok – „A regisztráció a bejelentőlap pontos kitöltését és a vendég személyazonosságának igazolását jelenti. A személyazonosító okirat bemutatása a hotel számára lényegesnek minősített szerződési feltétel...” – sok szállodai házirendben megtalálhatók, mégis csak elvétve látom, hogy alkalmazzák is ezeket. Feltételezem, nem szeretne senki kockáztatni azzal, hogy a vendég esetleg megsértődik a procedúra miatt, és sarkon fordul. Vagy lassítja a bejelentkezést az ellenőrzés? Esetleg a recepciósok számára kellemetlen? De akkor mi van a GDPR adatpontosságot előíró, 5. cikkével, vagy a turisztikai szabályozás idei módosításaival?

### VÁLOGATOTT SZABÁLYTALANSÁGOK

- Belépek a szállodába, sehol egy felirat a kamerás megfigyelésről. Esetleg van valahol egy pici piktogram.

Nem kell a falra, ajtóra ragasztani az erről szóló tájékoztatót, láttam már olyan elegáns megoldást, hogy az ajtónál helyeztek el egy szép megjelenésű kis állványt. A lényeg, hogy valahol meg kell jelenítenünk. A recepción már el se mertem kérni a kamerák elhelyezésével kapcsolatos ábrát vagy táblázatot...

- Lemegyek vacsorázni, és éppen senki nem áll az ajtóban, de a vacsoralista jól láthatóan ott van a pulton.

Sok jó megoldás van erre is, elhelyezhetjük például egy lecsukható dossziéban, ha éppen nincs ott senki.

- Több évvel ezelőtt az egyik kollégámmal, az ő autójával jártam egy szállodában, én csak mellé bejelentett vendég voltam. Amikor pár év múlva újra ott szálltam meg, a rendszer automatikusan feldobta a nevem mellé a kolléga régi autójának a rendszámát. Teljes képzavar volt!

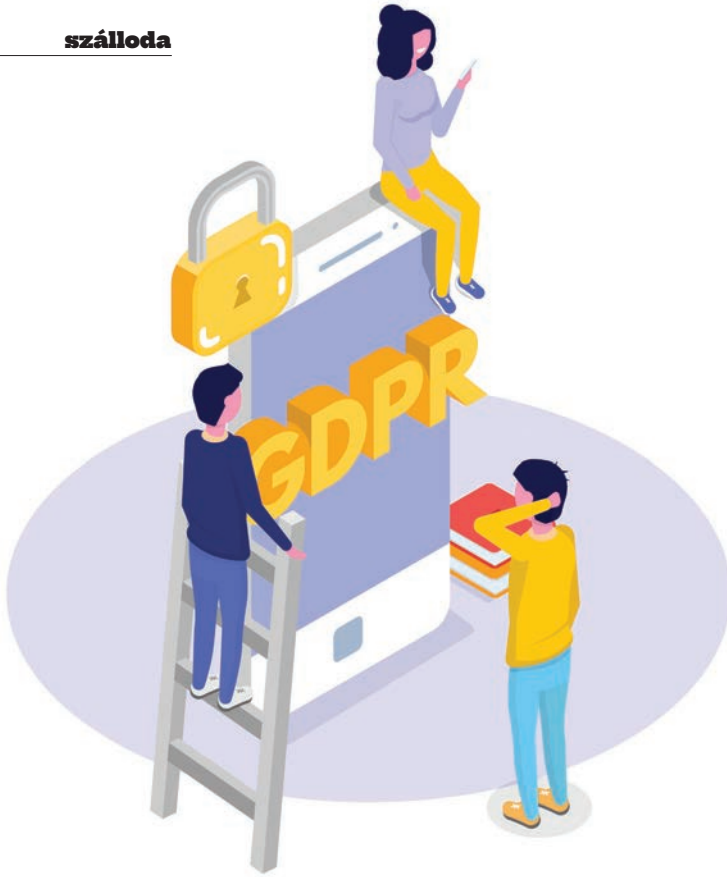
Ez ellen nem nagyon lehet mit tenni, mert szinte nincs is olyan szállodai szoftver, amelyből törölni lehetne a rendszámot, amikor az már nem kell. Remélem, a megoldás már úton van, mert egy nagyobb forgalmú szálloda adatállománya már olyan, mint egy kormányablaké!

- Az egyik szállodában a feleségem bediktálta a nevét, mire a recepciós azonnal rávágott egy születési dátumot (gondolom, mint azonosításra alkalmas adatot). A problémát az jelentette, hogy nem az ő, hanem egy 20 évvel idősebb hölgy születési adatai kerültek elő az adatbázisból.

Biztos jó pont a szállodának, ha régi ismerősként tud minket köszönteni. Azonban jobb, ha a recepciós előbb meggyőződik róla, hogy valóban azzal beszél-e, akire gondol. Ez egy adatbekérésből azonnal kiderül.

Mindig nehéz kitalálni, hogy mit csinálhatunk rosszul. A megoldás talán, hogy lássunk a GDPR mögé, miért is találták ki az egészet? Majd mérjük fel a kialakított, „GDPR-kompatibilis” rendszerünket, vizsgáljuk meg részegységenként, ellenőrizzük a napi működést, és a talált eltérések alapján fejlesszünk, mert mindig van mit. És nem utolsósorban, ha mindezekkel megvagyunk, tartsunk róla oktatást a munkatársainknak!

Egy bevezetett rendszerrel kapcsolatban az a legrosszabb, ha mi úgy gondoljuk, helyesen működik, a valóságban azonban mégsem.




# Papíralapon is dolgozunk!

**A GDPR-ról szóló cikksorozatom 8. részében nem a hazai szállodák informatikai állapotát boncolgatom, hanem egy „könnyedebb" témát járok körül, amely a GDPR-őrületben nagyjából a feledés homályába merült. Ez pedig az „örök" és elmaradhatatlan papír!**

Szerző: Makai Gábor, az MSZÉSZ GDPR-szakértője

Térjünk kicsit vissza az alapokhoz. Volt már ugyebár szó az „adatvagyonleltárról". Itt rögtön kiderül – ha jól csináltuk –, hogy milyen személyes adatokat őrzünk papíron, illetve, ha lelkiismeretesen állítottuk össze a leltárt, az is, hogy ezek a papíralapú dokumentumok kellenek-e még vagy sem (nyilván van, amit nem lehet kizárólag elektronikusan kezelni). Ugye tudjuk, ha nincs cél és jogalap, akkor nem lehetséges az adatkezelés, így a tárolás sem!

***KIFOGÁSOLHATÓ IRATHEGYEK*** Jogszabályi megfelelés céljából, valamint biztos, ami biztos alapon, megszokásból őrzünk minden iratot, amíg van hely az irattárban. „Bejelentőlapokat", számlákat, régi kérdőíveket, esetleg még névvel, címmel… Az iratok többségét ráadásul az „elődeink" hagyták ránk, pláne, ha hosszabb múlttal rendelkező szállodát üzemeltetünk. A selejtezés pedig egy olyan tevékenység, amelyre soha nincs sem idő, sem ember és talán módszertan sem.

Sajnos azonban a GDPR-rendelet az adatkezelő által kezelt személyes adatok összességére vonatkozik, tehát nem csak azokra, amelyek a rendelet hatálybalépése óta keletkeztek.

Első körben beszéljünk az „elfekvő" iratokról! Eddig nagyon kevés helyen találkoztam ezekre vonatkozó, megfelelően működő iratkezeléssel.

Érdemes megvizsgálni, hogy van-e iratkezelési szabályzatunk, illetve annak olyan része, amelyben pontosan meghatároztuk a selejtezési időket. Ez egyébként nem egyszerű feladat! Nagyon sok iratot törvényi megfelelés céljából kell megőrizni, a jogszabályi rendelkezések pedig néha nem egyértelműek, vagy pedig változnak.

Erre egy példa: a munkáltatók sokáig 50-70 évet határoztak meg a munkavállalók jogviszonyával kapcsolatos dokumentumok megőrzésére, mígnem 2018. december 23-i hatállyal megszületett az 1997. évi LXXXI. törvény kiegészítése, amelynek értelmében a munkáltatónak az öregségi nyugdíjkorhatár betöltését követő öt évig kell megőriznie az alkalmazottak szolgálati idejéről vagy keresetéről, jövedelméről adatot tartalmazó munkaügyi iratait. Jó hír! Lehet számolgatni és dossziékat feliratozni. Ha figyelembe vesszük, hogy van 22 éves és 56 éves munkavállalónk, továbbá hogy esetleg a nyugdíjkorhatár néhány éven belül megint változik, ez egy érdekes játék lehet.

***ELŐRELÁTÓAN DOSSZIÉZZUNK*** Ahol nincs jogszabályi előírás, ott a saját magunk belső szabályozása alapján, illetve most már a GDPR figyelembevételével (elavult cél és elavult jogalap) együtt kell meghatároznunk a selejtezési időket.

A napi munkamenetben pedig szükséges lenne egy olyan módszer kialakítása, amellyel úgy tudjuk dossziézni, rendszerezni és az irattárba tenni a dokumentumainkat, hogy azokat a megfelelő időpontokban selejtezni lehessen.

Tehát ha minden feltétel adott, akkor nem szabad tovább a homokba dugni a fejünket, muszáj nekiállni a selejtezésnek, mert ez is keményen a GDPR része. Két jó tanács: 1. a selejtezést dokumentáltan végezzük el és 2. az iratok legyenek ténylegesen megsemmisítve! Már sok rémhírt hallottunk a kukába, szelektív gyűjtőbe elhelyezett iratok utóéletéről. Ne adjunk esélyt a kukabúvároknak!

Egy személyes tapasztalatom a végére: szállodában vagyok a családdal, a szobában gyerekeknek szóló vicces kérdőívet találunk, amit mindenki örömmel tölt ki, mert este sorsolás és nyeremény. Gyerek neve és kora rákerül a papírra… Engem személy szerint nem zavart, de azt javaslom, ne hagyjunk támadási felületet a gyerekek adatai miatt. Egy szülői aláírás az alján mindent megoldana. Ha már vannak hasonló nyomtatványaink, akkor azokat is vizsgáljuk felül, és próbáljuk meg valahogy GDPR-kompatibilissé tenni.

Kalandra fel! Irány a padlás, irány az irattár! ❙

Fotó: 123rf.com

# Gyors körkép *A GDPR ALAPPILLÉREIRŐL*


**Kialakított GDPR-rendszerünk három fő alappilléren – jog, folyamatszervezés, információbiztonság – nyugszik. Ez a háromlábú szék bármelyik elem gyengesége miatt felborulhat. A GDPR-ról szóló cikksorozatunk 9. része következik.**

Szerző: *Makai Gábor, az MSZÉSZ GDPR-szakértője*

A felsorolt alappillérek közül a **jogi helyzet** már jónak mondható. Ennek oka, hogy mára a jogi feladatok elég jól körülhatárolhatóak, tisztulni látszik a kép a jogalkotók és az alkalmazók körében egyaránt. A „kirakatdokumentumok" elkészítésére, valamint a tevékenységére, a munkáltatói kötelezettségekre vonatkozóan, illetve a GDPR-rendeletet értelmező jogi alapkérdésekkel kapcsolatban szinte már mindenki kapott valamilyen „segítséget". Ennek volt a legegyszerűbb azonnal nekilátni, és ezt a területet tudta leginkább támogatni a sok-sok jogi tanácsadó is. A **szervezési területtel** csak módjával kezdtünk el foglalkozni. Ennek egyik oka, hogy sajnos a fontossága nincs kihangsúlyozva, az adatkezeléssel és a rendelettel összefüggő szervezési feladatokat általában senki sem veszi komolyan sehol, így ez szinte teljesen kimaradt a felkészülésekből, pedig lényegében a megfelelő adatkezelési módszer a működtetés gerince. A másik ok, hogy a GDPR által előírt kötelező tevékenységek kialakítása, illetve a napi adatkezelési rutinok, munkarendek meghatározása és bevezetése sok befektetett energiát igényel, sok időt emészt fel, és „szerencsére" egyelőre nincs közvetlenül a NAIH-vizsgálatok fókuszában. Pedig ettől is nagyot borulhat az a háromlábú szék!

## INFORMÁCIÓBIZTONSÁG: VEGYÜK MÉG KOMOLYABBAN

Az **információbiztonság** területével kapcsolatban jellemzően elképzelésünk sincs, hogyan állunk, aminek a legfőbb oka, hogy magával a fogalommal sem vagyunk tisztában, nem tudjuk pontosan, mit takar, és olyan egyszerű dolgokkal próbáljuk elintézni magunkban, mint „rendszergazda", „tűzfal" és „jelszó".
Hogy ki a felelős, esetleg hibás ezért? Szerintem messze nem Önök, ugyanis picit át is verjük ezzel kapcsolatban magunkat, hiszen az in-

Fotó: 123rf.com

formatika már jóval a GDPR-rendelet bevezetése előtt is jelen volt az életünkben, a mindennapjaink részévé vált, és már tudomást sem veszünk róla, csak ha baj van. Mivel ezzel azonosítjuk az információbiztonságot is, az a téves érzetünk támad, hogy minden rendben van vele! A GDPR bevezetésével együtt sem éreztünk rá az ezzel kapcsolatos pluszfeladatokra, pedig ez egy megfelelő löket és pillanat lehetett volna hozzá. Azonban még most sem késő, hogy átgondoljuk, újragondoljuk ezt a területet!

Vegyük észre, hogy az információbiztonsággal való komolyabb kapcsolat kialakítása a legmeghatározóbb és elkerülhetetlen tényező lett, mivel az adataink védelmét leginkább az informatikai rendszerünk biztonsága határozza meg, és az adatkezelési folyamataink már informatikai környezetben történnek.

A recepciónál számítógépre viszik az adatokat, amelyet a szerver tárol. A bejelentkezések, szobafoglalások internetes felületen érkeznek be hozzánk különböző motorok segítségével közvetlenül a szállodai szoftverünkbe, vagy e-mail formájában. Hírlevelek automatikusan mennek, e-mailek, űrlapok folyamatosan jönnek. A wellness-részlegen Excel-táblában rögzítünk adatokat, az okostelefonjainkon különböző adatkezelő applikációkat használunk.

Ráadásul szinte minden szállásadónál kihagyhatatlan tényező lett az informatikai rendszer alkalmazása, hiszen az NTAK-nak digitálisan kell beküldeni az adatokat, illetve a napi rutin is lassan elképzelhetetlen számítógép és IT-infrastruktúra nélkül.

Nagyon nehéz meghatároznia azt egy szervezetnek, legyen az szállodalánc vagy panzió, hogy mekkora energiát, pénzt és más erőforrást kell belefektetnie az információbiztonságba. Mert mit is jelent ez? Hol is kezdje el? Milyen lépései vannak? A következő cikkemben kísérletet teszek arra, hogy pár fogást bemutassak erre vonatkozóan. **I**

# INDUL AZ INFORMÁCIÓBIZTONSÁG

Húsz évvel az ezredforduló után már teljesen természetes számunkra, hogy az információs technológia átszövi a mindennapjainkat, megkönnyíti a munkánkat, a kommunikációt és egyáltalán az életünket, ezért is használjuk már olyan egyszerűséggel, mint egy kenyérpirítót. És talán ezért is kezeljük olyan nagyvonalúan és hanyagul a biztonságos használat kérdését. Pedig a kenyérpirítónak is van használati utasítása és biztonsági előírásai, amelyeket betartunk. A GDPR-ról szóló cikksorozatunk 10. részében ezt a kérdést járjuk körül.

Szerző: Makai Gábor, az MSZÉSZ GDPR-szakértője

Az információtechnológia biztonságával kapcsolatban gyakran elhangzanak olyan mondatok, mint „hogyan is tudnának hozzáférni az adataimhoz, hiszen azok védve vannak", ráadásul „a gépem itt van a nappalimban, a telefonom pedig a zsebemben, és még az ujjlenyomatom is védi az adatokat". Ez otthon valóban így is van, de mi a helyzet a munkahelyen? Rendre az a tapasztalat, hogy a cégeknél nagyobb a baj, mert több az adat, többen kezelik azokat, és sajnos alacsonyabb az információbiztonság-tudatosság szintje is.

Az előző cikkemben megígértem, hogy írok pár gondolatot a témával kapcsolatban. Hol is érdemes elkezdeni az információbiztonság fejlesztését, milyen lépései vannak?

Ezek közül az első és talán a legfontosabb, hogy a szállodaigazgatók és más turisztikai vállalkozások vezetői legyenek tökéletesen tisztában az információbiztonság fontosságával, és teljes elkötelezettséggel álljanak ki az adatvédelem mellett. Csak így tudják véghezvinni a szükséges változtatásokat.

A következő feladat a megfelelő intézkedések bevezetése. Na, itt a legtöbb helyen el is akad a dolog. Hogy miért? Biztosan tapasztalták már, hogy ha egy olyan új intézkedést vezetnek be, ami picit is „kényelmetlenebbé" teszi a munkavállalók napi életét, rögtön jönnek a megjegyzések és az ellenállás. Feltételezem, volt már részük hasonlóban. Gondoljunk csak az olyan újításokra, mint a csomagellenőrzés, a belépőkártya vagy a havi jelszócsere bevezetése. Ugye, egyik sem volt zökkenőmentes? És akkor a titkosításról vagy a kétlépcsős azonosításról még nem is beszéltünk... Sajnos nincs jó hírem, ez is egy olyan fal lesz, amelyet Önöknek kell áttörniük.

Érdemes megkérdezni a kevésbé együttműködő munkatársakat, hogy például a saját autójuk biztonságával kapcsolatos intézkedések nem kényelmetlenek-e a számukra? Az autóban hajlandóak matatni az „esernyős" vagy a kormányra szerelhető „csodavédelemmel", a sebváltózárral, vagy a titkos kapcsolóval, amelyet a jobb kezükkel a bal fülük felett átnyúlva kell megnyomni, miközben szól a rádió és nyomják a fékpedált... Tehát ott, ahol akarják, és nekik számít, belefér a plusz „kényelmetlen" helyzet? Máshol meg nem? Pedig mennyivel egyszerűbb lenne csak úgy bepattanni a nyitott ajtóval járó motorú kocsiba. A legtöbben ilyen hanyagul kezelik az IT-rendszereiket.

Különösen fontos feladat, hogy az intézkedések bevezetésével párhuzamosan kerüljön sor a kapcsolódó oktatásokra, képzésekre annak érdekében, hogy a munkatársak megszerezzék azt az általános és szervezetspecifikus információbiztonsági tudást, amelynek birtokában megértik, hogy miért is van szükség az intézkedésekre. Továbbá ezt a tudatosságot és tudást ne feledjék el folyamatosan fenntartani!

## Mennyit áldozzunk rá?

A megfelelő IT-szakember kiválasztása sem könnyű feladat. Sajnos nem igazán figyelünk erre, mert amíg jól működik minden, azt hisszük, hogy nincs is rá szükség, pedig pont fordítva van: azért van rá szükség, hogy minden rendben működjön. Ha van rá lehetőségünk, akkor válasszuk külön a nyomtatópatront cserélgető, mosolygós rendszergazdát az IT-hálózat- és szerverüzemeltető kollégától.

Honnan tudjuk, hogy ki a jó IT-üzemeltető? Majdnem sehonnan, mert ameddig nincs baj, addig nem derül ki. Mindenesetre jó, ha tud szolgálni információval a fejlesztési lehetőségeinkről, a jelenlegi kockázatainkról, azok megoldásairól, valamint naprakész tudása és tapasztalata van. Ha megtaláltuk a megfelelő embert, akkor kommunikáljunk vele rendszeresen, és ha fejlesztési javaslatai vannak, akkor legyünk azokra nagyon nyitottak, hiszen az ő tudása és tapasztalata meghatározó lesz a munkahelyen.

És persze adódik a legnehezebb kérdés, ami napjainkban valószínűleg kiemelkedően érzékeny terület: mennyit költsünk az információbiztonságra? Ezt megmondani persze nem lehet, de segítségképpen az a javaslatom, gondolják át, hogy a saját gépjárművükre mennyi cascót fizetnek, mennyit költenek a védelmi rendszerére és az üzemeltetésére. Ezt a százalékot vetítsék rá a szálloda nyereségére, hírnevére, adatainak értékére stb., és akkor kapnak egy olyan számot, amelyet kiindulási alapnak lehet tekinteni.

Hogy hol állnak most információbiztonság területén, azt csak egy átfogó szakmai ellenőrzés tudja megfelelő pontossággal megmondani. Léteznek felkészült szakemberek, cégek, akik, illetve amelyek ebben a segítségükre lehetnek. Ha módjuk adódik rá, egyszer próbáljanak ki egy ilyen átvilágítást, meglepő, ám annál használhatóbb és már rövid távon is kifizetődő eredményeket kaphatnak. ❙

# A GAZDASÁG MEGTORPANT, DE A GDPR NEM TŰNT EL…

Szerző: Makai Gábor, az MSZÉSZ GDPR-szakértője
Fotó: 123rf.com

**Több mint egy évvel ezelőtt indítottuk útjára az uniós adatvédelmi rendeletről szóló, tízrészes cikksorozatunkat, amelyben azt jártuk körül, hogy milyen szempontokat érdemes figyelembe venniük a turisztikai vállalkozásoknak a GDPR-megfelelőségi rendszer kiépítése során. Akkor még nem is sejthettük, hogy a sorozat befejező cikke különösen nehéz gazdasági-társadalmi körülmények között jelenik majd meg – egy olyan időszakban, amikor talán még fontosabb az adatok védelme, mint volt bármikor előtte.**

Nehéz szívvel álltam neki a befejező rész megírásának, hiszen tudom, hogy ma Magyarországon az önöké az egyik olyan szektor, amelyet a leginkább sújtanak a koronavírus-járvány miatti korlátozások.
A turizmusban ez most a túlélés, a jövőért való küzdelem és a visszarázódás időszaka, így nem csodálkozom azon, hogy mostanában picit háttérbe szorult a GDPR, vagy legalábbis nem ez a legkiemeltebb téma. Gondolom, az elmúlt időszakban önöket sem az érdekelte elsősorban, hogy a cégük működése GDPR-kompatibilis-e vagy sem…
A nehézségek azonban sajnos nem mentesítenek senkit a GDPR-nak való megfelelés alól. Pláne, hogy a szervezetek épp „káoszban” a legsérülékenyebbek, hiszen az ehhez hasonló időszakokban nem az adatvédelem a legfontosabb szempont, amire bárki is gondol.
A koronavírus-járvány miatt előállt helyzet a GDPR-megfelelés mindhárom alappillérét – jog, folyamatszervezés, információbiztonság – nagyban érinti. Engedjék meg, hogy búcsúzásként ezt illusztráljam néhány példával:

## Jogi környezet

Nézzük csak meg a http://net.jogtar.hu/veszelyhelyzet linken található listát, hogy a veszélyhelyzet miatt hány jogszabályhoz, rendelethez kellett hozzányúlni, illetve hány újat kellett megalkotni szinte pillanatok alatt. Ember legyen a talpán, aki ezekből pontosan ki tudja szedni az adatkezelési vonatkozásokat, pedig vannak bőven! Vagy megnézhetjük a NAIH 2020/2586. számú tájékoztatását is a koronavírus-járvánnyal kapcsolatos adatkezelésről. Gondoljunk csak azokra az esetekre, amikor „COVID–19 kérdőíveket” kellett kitölteniük a munkavállalóknak, belépőknek, vagy egy-két szállodában az érkező vendégeknek. Ezekben csak úgy záporoznak a személyes, illetve a kiemelten személyes adatokra vonatkozó kérdések. Vajon mindenki pontosan tudja az új rendelkezések alapján, hogy mely adatokat lehet regisztrálni és melyeket nem? Vagy akár azt, hogy adott esetben lehet-e lázmérőt alkalmaznia a munkáltatónak?

## Munkaszervezés

Természetesen tudom, hogy az ilyen és hasonló történésekre nem nagyon gondolt senki az üzletmenet-folytonossági tervében. Az első időben amiatt is nagy volt a kapkodás, hogy a szállodák nem a home office típusú munkavégzésre optimalizálták a működésüket, így biztos vagyok benne, hogy okozott némi fejtörést, hogyan oldják meg ezt a helyzetet mind a munkaszervezés, mind pedig az IT oldaláról. A fenntarthatóság érdekében valószínűleg kénytelenek voltak a biztonsági elveiket félretéve megtalálni az azonnali megoldásokat…

## Informatikai és IT-biztonság

Nagyon fontos feladat lett az adatok mozgatása, a biztonságos kapcsolatok kiépítése, az eszközök biztosítása, az adathordozók szállításából fakadó kockázatok kezelése.
A korlátozások után, az otthoni időszak lezárását követően pedig ellenőrizni kell az adatokat, amikor az visszakerül az adatkezelőhöz, mivel a GDRP 32. cikke elvárja az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását, függetlenül attól, hogy a munkatársak home office-ban vagy az irodában látják el a feladataikat.

### *EMLÉKEZTETŐ*

Az elmúlt egy évben a GDPR-megfelelőségi rendszer számos összetevőjét tekintettük át.
Cikksorozatunk a Turizmus.com 2019/4. számában indult el néhány gondolatébresztő felvetéssel.
Következő lapszámunkban megvizsgáltuk, hogy feltétlenül szükséges-e mindig alkalmaznunk a hozzájárulást mint jogalapot, és kiderült, hogy nem mindig ez a legegészszerűbb megoldás (2019/5.).
Egy hónappal később segítséget kaptunk az adatvagyonleltár összeállításához, amely az egész megfelelőségi rendszer alapja, ennek hiányában nem tudjuk a rendszert sem felépíteni, sem működtetni (2019/6.).
Majd a jogosultsági rendszer kiépítésével folytattuk, amelyre az információbiztonság alapkövetelményének (miszerint az információ csak az arra felhatalmazottak számára legyen elérhető) teljesítése miatt van szükség (2019/9.).
Az üzletmenet-folytonossági rendszer kiépítése pedig ahhoz ad segítséget, hogy garantálni tudjuk a kockázat mértékének megfelelő szintű adatbiztonságot (2019/10).
Foglalkoztunk a biztonsági kamerák működtetésének buktatóival is (2019/11.).
Decemberi lapszámunkban szembesültünk azzal, hogy a „kirakatintézkedések” csak látszatra biztosítják egy szervezet GDPR-kompatibilitását, sőt gyakran ezek is több sebből véreznek (2019/12.).
Majd a papíralapú dokumentumok kezeléséhez kaptunk ötleteket, amelyek nemritkán hegyekben állnak a cégek raktárában (2020/1-2.).
Márciusban azt vettük górcső alá, mennyire erős a GDPR három alappillére a hazai turisztikai vállalkozásoknál (2020/3.).
Végül – már jócskán a veszélyhelyzet idején – a leggyengébb pillér, az információbiztonság fontosságával foglalkoztunk behatóan (2020/4.).

Kívánok Önöknek sikeres talpra állást, zökkenőmentes újraindulást, sok vendéget és egy kiforrott, rutinszerűen működtetett GDPR-megfelelési rendszert! ❙

# GDPR: védettségi igazolvány és adatbiztonság

Az uniós adatvédelmi rendelet, a GDPR a Covid-19 elleni védettséget tanúsító igazolás kötelező ellenőrzése során is jelent némi pluszmunkát, szakértőnk ehhez ad néhány gyakorlati tanácsot.

Szerző: Makai Gábor GDPR-szakértő, Fotó: 123rf.com

Az utóbbi évtizedek egyik legnehezebb időszakát éltük meg az elmúlt közel másfél évben, legyen szó a munkahelyünkről, az egészségünkről, szeretteink biztonságáról. Ebben a helyzetben a szállodák, éttermek és a kapcsolódó piaci szereplők nemcsak érintettek voltak, de a legnagyobb mértékben sújtott ágazatok között szerepeltek.

És bár a biztonságérzet még nem érte el, és vélhetően egy ideig nem is fogja elérni a régi szintet, megkaptuk a zöld jelzést, eljött a pillanat, végre újra kinyithattuk a kapukat, és fogadhatjuk a vendégeket!

A figyelmünket eddig lekötötte a várakozás, a munkatársaink megtartása, a felújítások, az utolsó ablakok tisztogatása, és persze a tervezgetés, ám eközben vélhetően kevesebbet gondoltunk arra, hogy az adatkezelési rendszerünket miként befolyásolja majd a nyitás. Ezzel kapcsolatban szedtük össze a legfontosabbakat.

## Betekintés, adatrögzítés nélkül

Sokat segíti a munkánkat – hiszen így nem kell találgatni, tippelgetni –, hogy a 484/2020. (XI.10.) Korm. rendelet és annak módosításai, kiegészítései egyértelművé tették a szabályokat, sőt a NAIH is megerősítette, hogy a védettségi igazolvány bemutatása nem alkotmányellenes, mivel arról semmilyen adat nem rögzíthető, továbbá azt nem lehet lefotózni, lemásolni. Itt véget is érhetne a cikk, mert a rendelet elég pontosan meghatározza a teendőket, de azért tennék néhány kiegészítést az adatkezelésre vonatkozóan.

Talán a legfontosabb, hogy a védettségi igazolványt valóban ellenőrizni kell, mert ellenkező esetben komoly bírság várhat ránk.

A GDPR szempontjából könnyű a dolgunk, mert a fent említett rendelet máris megfelelő és biztos jogalapot adott az adatkezeléshez, amely tehát a GDPR. 6. cikk (1) bekezdés c) pontja alapján jogi kötelezettség teljesítése céljából történik. Azt illetően, hogy a szálláshely képes legyen megfelelni az elszámoltathatóság elvének és igazolni tudja azt, hogy az igazolvány megtekintésével kapcsolatban megtett tőle minden telhetőt, már nehezebb helyzetben vagyunk, hiszen a rendelet értelmében a védettségi igazolás megtekintésének tényét semmilyen módon nem lehet rögzíteni, dokumentálni. Nem tehetünk zöld pipát a bejelentőlapra, nem készíthetünk egy kis jelölőnégyzetet a szoftverünkben erre vonatkozóan. Mint minden esetben, itt is vannak kivételek, ugyanis, ha a vendég tartózkodása üzleti, gazdasági, oktatási célú, vagy a Magyar Honvédség, illetve rendvédelmi szervek állományába tartozó személyként vagy egészségügyi dolgozóként szolgálatteljesítés céljából kíván a vendég megszállni, úgy a szálláshelyen történő tartózkodásnak nem feltétele a védettségi igazolvány bemutatása. Az ebbe a kategóriába tartozó vendég a szálláshelyen ta-

lálható wellnessrészleget (uszoda, fürdő, fitneszterem stb.) azonban csak abban az esetben jogosult használni, ha a koronavírus ellen védett személynek minősül. Ennek igazolására felszólíthatjuk őt.

A szálláshelyen a koronavírus ellen védett személy, valamint a felügyelete alatt álló, 18. életévét be nem töltött személy tartózkodása megengedett. Ha a szálláshelyre érkező külföldi állampolgár rendelkezik olyan ország által kiállított védettségi igazolással, amely ország által kibocsátott védettségi igazolást Magyarország elismeri, és ennek tényét a külpolitikáért felelős miniszter a határrendészetért felelős miniszterrel egyetértésben kiadott rendeletében megállapította, és a koronavírus elleni védettségét a részére kiállított koronavírus elleni védettségi igazolás bemutatásával igazolja, akkor fogadható a szálláshelyen. A szálláshelyen a védettségi igazolvánnyal rendelkező külföldi állampolgár felügyelete alatt álló, 18. életévét be nem töltött személy is fogadható. A szálláshelyeken fogadható továbbá olyan külföldi személy is, aki üzleti, gazdasági célból érkezett Magyarország területére.

Ne feledkezzünk meg arról sem, hogy a védettségi igazolvány mellett ellenőrizhető az azt felmutató személy személyi azonossága, valamint az életkora, de „szerencsére" erre a rendelet felhatalmaz bennünket. Ismételten hangsúlyoznám az alapos ellenőrzés fontosságát, mert egyrészt kétféle védettségi igazolvány létezik, az egyik az oltás tényét igazolja, a másik azonban azt, hogy valaki átesett a Covidon, ez utóbbi igazolványon azonban lejárati idő is szerepel. Vagyis az, hogy rutinszerűen rápillantunk az igazolványra, nem elegendő! Nem szemezgetnék a rendelet további részleteiből, de mindenképpen ajánlott olvasmány, amiből azt is megtudhatjuk, hogy jogunkban áll (sőt kötelező) a szolgáltatás megtagadása bizonyos esetekben.

A gyakorlatban tehát az elsődleges tennivaló, hogy betartsuk a most hatályban lévő vészhelyzeti rendeletet. Az, hogy került bele egy kis adatkezelés, csak hab a tortán, de nem kell megijedni tőle, és főképp nem kell túlzásba vinni. A rendelet jelenleg „csak" azt mondja ki, hogy ellenőriznünk kell a szállodába belépő vendégek „védettségét", illetve, hogy ennek eleget tudjunk tenni, a személyazonosságot is. Ez utóbbi nem is jelenthet gondot, mert a szállodai bejelentkezéseknek elvileg ez már régóta „kötelező" eleme. Adatkezelés a NAIH szerint lehetséges, mert nincs adatrögzítés, csupán „betekintés" (ugyebár már ez is adatkezelés). Ezzel nem végzünk felesleges adatkezelést, illetve bizonyítható az ellenőrzés ténye. Ez semmilyen plusz adatkezelést nem jelent az érintettre vonatkozóan, illetve ne felejtsük el, hogy törvényi megfelelés érdekében tesszük mindezt.

## Adatkezelési tájékoztató és eljárásrend

Az adatkezelési tájékoztató kiegészítése feltétlenül szükséges lesz erről az adatkezelésről, és nem árt módosítani azt az adatkezelési eljárásrendünket sem, amit a bejelentkezéssel kapcsolatos adatkezeléshez készítettünk, így biztos, hogy a munkatársaink is tisztában lesznek az egyértelmű elvárásokkal, szabályokkal, amelyeket követniük kell.

## Tájékoztatás

Mivel ez egy újdonság mindenki számára, érdemes és javasolt minél több helyen, lehetőleg mindenről tájékoztatni a vendégeket! A weboldalon, a bejáratoknál, a recepciónál ki kell tenni egy rövid ismertetőt, ami az adatkezelés jogosságára, annak kötelezőként történő bevezetésére, illetve az új helyzetből adódó esetleges kellemetlenségek elkerülésére hívja fel a figyelmet. Javaslom, hogy rendszeresen figyeljék a veszélyhelyzettel kapcsolatos, elég sűrűn megjelenő rendeleteket, szabályozásokat, mert ez most az az időszak, amikor napról napra bármi változhat. Kérjék jogászaik vagy GDPR-tanácsadóik segítségét, mert biztos lesznek még olyan módosítások (akár a kiskorúak oltására gondolunk, akár arra az időszakra, amikor ez az egész véget ér), amelyek változtatni fognak a bevezetett módszereken. ❙

*Kérdések esetén továbbra is rendelkezésükre állok az alábbi elérhetőségen: makai@euline.hu*

# turizmus.com

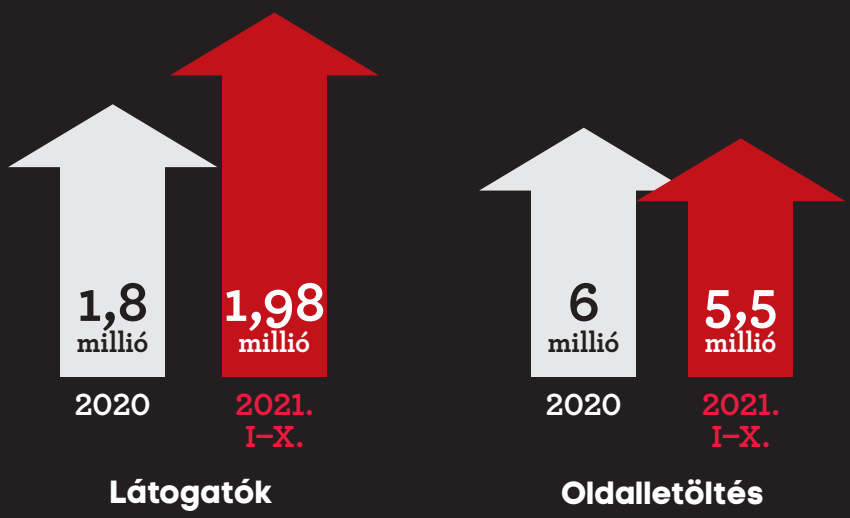
## A TURISZTIKAI SZAKMA HÍRFORRÁSA

Folyamatosan frissülő
**hírfolyam**

A szakma meghatározó
szereplőinek **adatbázisa**

**Állások**
a turizmusban

## LEGYEN A TURIZMUS.COM **NÖVEKVŐ** KÖZÖSSÉGÉNEK TAGJA!




**Kérje ingyenes napi hírlevelünket,**
**A TURIZMUS.COM BULLETINT!**

**Hirdetési ajánlatunkért keresse kollégáinkat: sales@turizmus.com**