Hazai normatív környezet

1. Létrejött az NVVH, rengeteg törvény emiatt módosul

A 2026. évi XXXIV.tv.-ben, mely 2026.07.29. napjától lépcsőzetesen lép hatályba, a közbizalom helyreállítása és a közélet tisztaságának megerősítése érdekében az Országgyűlés létrehozta a Nemzeti Vagyonvisszaszerzési és Vagyonvédelmi Hivatalt (NVVH), amely független, kizárólag a törvénynek alárendelt központi költségvetési szervként működik. A törvény több tucat jogszabályban teremt a hivatal számára jogköröket, így érinti a munka törvénykönyvét, egyéb foglalkoztatási jogszabályokat, a pénzügyi szervezetekre vonatkozó szabályokat, a versenyjogi szabályozást, az egyenlő bánásmód szabályozást, a kibervédelmi törvényt, valamint a pénzmosás szabályozását stb.
Hatályos: 2026.07.29. napjától lépcsőzetesen

Megszűnik az SZTFH

2. Átvilágítják az SZTFH működését annak megszüntetését megelőzően

A kormány megvizsgálja a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH), illetve a szervezet működését meghatározó törvényeket. A hatóságot megszüntetné, és feladatait szétosztaná állami szervek között. A miniszterelnök az igazságügyi minisztert bízta meg, hogy szeptember végéig tegyen javaslatot, milyen szabályozási megoldások szükségesek a szervezet megszüntetéséhez, és a hatáskörök elosztására a már meglévő állami szervek között. 2021-ben hozta létre az előző kormány az SZTFH-t, és egymástól teljesen független területek felügyeletével bízta meg. A szervezet kapta egyebek mellett a dohánytermékek piacának, a Magyar Bírósági Végrehajtói Karnak, a szerencsejátékok és bányák felügyeletét, a felszámolói névjegyzék vezetését, valamint a koncessziós szerződésekben szabályozott tevékenységek ellenőrzését. Ezekben egy közös vonás van: mindegyiket sok kritika érte a politikai összefonódások miatt. A felügyelet önálló szabályozó szervként csak az Országgyűlésnek tartozott beszámolási kötelezettséggel. Az SZTFH függetlenségét megkérdőjelezi, hogy élére a Miniszterelnöki Kormányiroda korábbi közigazgatási államtitkárát nevezték ki, kilenc évre. Vezetői tisztségeire nem kellett pályázatot kiírni.

Dokumentációs hiányosságok NIS2 auditoknál

3. Lezárult a kiberbiztonsági auditok határideje

Újabb fontos mérföldkőhöz érkezett a hazai NIS2 szabályozás végrehajtása, ugyanis 2026. június 30-ig kellett az auditkötelezett szervezeteknek lefolytatniuk kiberbiztonsági auditjukat. A Hatósághoz beérkezett adatok alapján az érintett szervezetek túlnyomó többsége határidőben teljesítette kötelezettségét, az eddig feldolgozott auditjelentések pedig azt mutatják, hogy a szervezetek jelentős része sikeresen megfelelt az előírásoknak. Az auditorok tapasztalatai szerint a vezetői elkötelezettség és a megfelelő szakmai felkészültséggel rendelkező információbiztonsági felelősök kulcsszerepet játszanak a sikeres megfelelésben. 2026. június 30-ig összesen 2194 szervezet teljesítette az első kiberbiztonsági auditot. Az érintett szervezetek közel 90%-a sikeresen megfelelt az audit követelményeinek, mintegy 10%-uk pedig a legmagasabb értékelést, az „Elhanyagolható kockázattal megfelelt” minősítést kapta.

Számos intézkedés segíti a fenntarthatóságot

4. Fogyasztóvédelem, zöld átállás

Az **áruk javításának előmozdítását célzó intézkedésekről** és egyes fogyasztóvédelmi tárgyú kormányrendeletek módosításáról szóló **114/2026. (VII.23.) korm.r.**, mely **2026.08.31. napjától** lépcsőzetesen lép hatályba, célja az áruk javításának ösztönzése a fenntartható fogyasztás előmozdítása, az erőforrás-felhasználás és az üvegházhatású gázok kibocsátásának csökkentése érdekében. Meghatározza a fogyasztók által vásárolt áruk javítására vonatkozó szabályokat, bevezeti az önkéntesen alkalmazható európai javítási adatlapot, előírja a gyártók javítási kötelezettségét az uniós jogi aktusokban meghatározott javíthatósági követelmények esetén, biztosítja a pótalkatrészek elérhetőségét, valamint a javításhoz szükséges információkhoz és eszközökhöz való hozzáférést. A rendelet lehetővé teszi, hogy a fogyasztók független javítószolgálatokat is igénybe vegyenek, és csatlakozik az európai online javítási platformhoz. Hibás teljesítés esetén a javítás választása esetén a kellékszavatossági igény elévülési ideje egyszer 12 hónappal meghosszabbodik. A jogszabály összesen két meglévő jogszabályt módosít: a 373/2021. (VI. 30.) Korm. rendeletet és a 326/2024. (XI. 14.) Korm. rendeletet.
A fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014. (II. 26.) Korm. rendelet módosításáról szóló **116/2026. (VII.30.) korm.r.** **2026.08.02. napjától** lépcsőzetesen lép hatályba. A rendelet célja, hogy a zöld átállás előmozdítása érdekében a fogyasztók megalapozottabb vásárlási döntéseket hozhassanak, ezzel támogatva a fenntarthatóbb fogyasztási szokások

kialakulását. Ennek érdekében előírja, hogy a vállalkozások a szerződéskötést megelőzően minden árutípus esetében külön tájékoztatást nyújtsanak a termék tartósságáról és javíthatóságáról, továbbá bevezeti a tartósságra vonatkozó kereskedelmi jótállás, a javíthatósági pontszám, valamint a harmonizált értesítés és címke fogalmát. A fogyasztók számára kötelezően közérthető és világos tájékoztatást kell adni többek között a tartósságra vonatkozó jótállásról, a szoftverfrissítések időtartamáról, a javíthatósági pontszámról, illetve a pótalkatrészek elérhetőségéről és a javítási lehetőségekről. A rendelet módosítja a szerződéses tájékoztatási kötelezettségeket, valamint az elállási és felmondási mintatájekoztatót, továbbá harmonizálja a hazai szabályozást az uniós jogszabályokkal, különös tekintettel a fogyasztók zöld átállásban való szerepvállalásának elősegítésére és a tisztességtelen kereskedelmi gyakorlatok elleni védelemre.
Végezetül fogyasztóvédelmi tárgyú törvényeknek a mikro-, kis- és középvállalkozások támogatását és jogharmonizációt célzó módosításáról szóló **2025. évi XCIV.tv.** módosítja **2026.09.27. napjától** a **fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmá**ról szóló 2008. évi XLVII.tv-t. A jogszabályváltozás a zöld állításokat szabályozza, a törvénybe beépül az áru, a digitális elemeket tartalmazó áru, az elismert kiváló környezetvédelmi teljesítmény, a fenntarthatósági címke, a fogyóeszköz, a funkcionalitás, a környezetbarát jellegre vonatkozó állítás, a környezetbarát jellegre vonatkozó általános állítás, a szoftverfrissítés, a tanúsítási rendszer és a tartósság fogalma. Emellett újabb 12 ponttal egészül ki a tisztességtelen kereskedelmi gyakorlatok listája. A tisztességtelen zöld állításokat a GVH is ellenőrzi.

5. Változó termékfelelősségi szabályok

A **2025. évi XCII.tv.** 2026.12.9. napjával változtat a termékfelelősség Ptk-ben rögzített szabályain. Az (EU) 2024/2853 irányelv hatályon kívül helyezi 85/374/EGK tanácsi irányelvet, valamint modernizálja a termékfelelősségi szabályokat, ezért volt szükséges a Ptk. termékfelelősségről szóló szabályainak áttekintése és módosítása. A termékfelelősségi szabályok modernizálásának célja, hogy a jogi keret a körforgásos gazdaság üzleti modelljeihez, a digitális kor termékeihez igazodjon, továbbá egyenlőbb versenyfeltételeket teremtsen az európai uniós és unión kívüli gyártók számára, valamint a károsultak gyártókkal szembeni igényérvényesítését megkönnyítse.
Hatályos: 2026.12.09.

6. Közigazgatási digitalizáció és fogyasztóvédelem

A **2026. évi LIV.tv.** célja a magyar közigazgatás digitalizációjának előmozdítása, a vállalkozások és fogyasztók közötti egyensúly erősítése, valamint a fenntartható fogyasztás támogatása, különös tekintettel a fogyasztók zöld átállásban való szerepvállalásának növelésére. A jogszabály két meglévő törvényt módosít: egyrészt meghatározza, hogy az egyes adótörvények adminisztrációt csökkentő és jogharmonizációs célú módosításáról szóló 2025. évi LXXXIII. törvény több szakasza 2028. január 1-jén lép hatályba, másrészt rendelkezik arról, hogy a fogyasztóvédelmi tárgyú törvényeknek a mikro-, kis- és középvállalkozások támogatását és jogharmonizációt célzó módosításáról szóló 2025. évi XCIV. törvény 12. §-a nem lép hatályba. A törvény az (EU) 2024/825 irányelvnek való megfelelést is biztosítja.
Hatályos: 2026.09.19, 09.27.

7. Igazságügyi tárgyú törvények: megszűnik a tárgyalások online nyilvánossága

Az egyes igazságügyi törvények módosításáról szóló 2026. évi LIII.tv. 2026. november 18. napjától lépcsőzetes hatályba lépéssel hatályon kívül helyezi a bírósági tárgyalások online nyilvánosságára vonatkozó jogszabályi rendelkezéseket (15/2025. (XII.10.) IM rendelet). A tárgyalás online nyilvánossága megteremtésének eredeti célja a társadalmi kontroll kiterjesztése, valamint a jogi oktatás és kutatás támogatása voltak. E célok azonban önmagukban nem igazolták a szabályozás fenntartását, mely veszélyeztette a bizonyítás zavartalanságát, a személyes adatok védelmét és a bíróságok megfelelő működését. Emellett változik a peres eljárás szabályozása is elsősorban a közéleti részvételt akadályozó, visszaélésszerű bírósági eljárások kapcsán. Emellett pontosítja a hibás termékekért való felelősség szabályait, valamint a szavazatelsőbbségi részvénystruktúrákra és a nemzetközi magánjogi eljárásokra vonatkozó harmonizációs rendelkezéseket.
Hatályos: 2026.11.08. napjától lépcsőzetesen

8. TAKARNET online időpontfoglalás

Éjjel-nappal elérhető, egyszerű és gyors online időpontfoglaló rendszer segíti a Takarnet ügyfélszolgálatához kapcsolódó hatósági bizonyítványi ügyek intézését. A Lechner Tudásközpont oldaláról elérhető új felületen néhány kattintással lefoglalható, módosítható vagy lemondható az

időpont, így az ügyintézés még gördülékenyebb és kiszámíthatóbb. A rendszer automatikus visszaigazoló e-mailt küld a foglalásról. A hatósági bizonyítványhoz kapcsolódó ügyintézési idősávok: Hétfő: 8:30–12:00, Szerda: 13:00–16:00, Péntek: 8:30–11:00. Amennyiben az időpontfoglalás során kérdés merül fel, vagy segítségre van szüksége, ügyfélszolgálatuk a +36 1 279 2640 központi telefonszámon érhető el.

9. Újabb DÁP funkciók érhetőek el

Több újabb DÁP funkció elérhetővé vált. Keresési előzmények a szűrőknél és a naplónál: A mindennapi használat megkönnyítése érdekében a rendszer – a böngésző támogatásával – megjegyzi a korábban használt keresési és szűrési kifejezéseket, így kevesebb időt kell ugyanazon feltételek ismételt megadásával tölteni. A funkció a Beérkezett üzenetek, a Tartós tár és az Elküldött üzenetek felületein, valamint a Napló használata során lesz elérhető. Fiókválasztó, olvasatlan üzenetek automatikus frissítése: A fiókválasztó lenyitott állapotában az egyes fiókokhoz tartozó olvasatlan üzenetek száma automatikusan frissül. Ennek köszönhetően mindig naprakész információ áll rendelkezésre anélkül, hogy a felületet újra kellene tölteni. Kiemelten figyeltek arra is, hogy az automatikus frissítés ne zavarja meg a folyamatban lévő műveleteket. Így, ha éppen egy fiók megjelenítési nevét szerkesztik, a háttérben futó frissítések nem szakítják meg a munkafolyamatot, így a módosításokat fennakadás nélkül végezhető el. Végül elindult a DÁP Facebook oldala is.

10. Bírósági döntések

HR

BH2026.175: Szabadság elévülése

A szabadság kiadására vonatkozó igény elévülése mindaddig nyugszik, amíg a munkavállaló azt menthető okból nem tudja érvényesíteni. Menthető oknak minősül az, hogy a munkáltató munkaszervezési okra hivatkozva nem adja ki a tárgyévi szabadságot teljes egészében. (A szabadság elévülése ilyenkor a munkaviszony megszűnésével kezdődik.)

BH2026.138. Vezető állású munkavállalói státusz

Az Mt. 208. § (1) bekezdésében foglaltak konjunktív feltételek, amelyek közül bármelyik hiánya azt eredményezi, hogy az adott munkakörben foglalkoztatott munkavállaló nem tekinthető e rendelkezés alapján vezető állásúnak. Az Mt.208.§ (1) bekezdése alapján vezető állású munkavállaló a munkáltató vezetője, valamint a közvetlen irányítása alatt álló és – részben vagy egészben – helyettesítésére jogosított más munkavállaló (a továbbiakban együtt: vezető). A (2) bekezdés szerint azonban munkaszerződés a vezetőre vonatkozó rendelkezések alkalmazását írhatja elő, ha a munkavállaló a munkáltató működése szempontjából kiemelkedő jelentőségű vagy fokozottan bizalmi jellegű munkakört tölt be és alapbére eléri a kötelező legkisebb munkabér [153. § (1) bekezdés a) pont] hétszeresét. Ehhez kapcsolódóan a Kúria rámutatott arra, hogy a felperes ugyan az ügyvezető közvetlen irányítása alá tartozott, arra nézve azonban nem volt sem okirati, sem egyéb adat, hogy annak helyettesítésére lett volna feljogosítva. Az alperesnek lehetősége volt a helyettesítés rendjét szabályozni, amely a felperesre is kihatott volna, ezt azonban elmulasztotta. Nem vitásan a felperes bizonyos döntések előkészítésében részt vett, a végső döntés meghozatalára azonban csak az ügyvezetőnek volt hatásköre. Az alperes maga sem állította, hogy felepres munkaköri feladatai, hatásköre, felelőssége alapján első számú vezetőnek minősülne. Munkaszerződésben foglalt megállapodás hiányában pedig nem volt vizsgálható, hogy a munkáltató működése szempontjából kiemelkedő jelentőségű vagy fokozottan bizalmi jellegű munkakört látott-e el (Mt. 208. § (2) bekezdés).

Adatvédelem

BH2026.164.: A személyes adattal való visszaélés büntetőjogi következményei

A személyes adattal visszaélés vétségének a Btk. 219. § (1) bekezdés a) pontjában írt esete megvalósulásának feltétele, hogy a jogosulatlan vagy céltól eltérő személyes adatkezelés jogtalan haszonszerzési célból valósuljon meg, vagy az a jogalap nélküli adatkezeléssel összefüggésben az érintett személynek jelentős érdeksérelmet okozzon.

BH2026.152. Az adatfeldolgozó fogalma

Az adatfeldolgozó fogalmának értelmezésekor azt kell vizsgálni, hogy a feladatait az adatkezelő nevében, a személyes adatokat az adatkezelő által meghatározott célból, az adatkezelő érdekében és az adatkezelőtől elkülönült jogalanyként, az adatkezelést érintő érdemi döntési jogosítványok nélkül végzi-e.

Tisztességtelen kereskedelmi gyakorlatok

BH2026.119.Tisztességtelen kereskedelmi gyakorlat: fizetés visszatérítésének módja
Miután a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014. (II. 26.) Korm. rendelet 23. § (2) bekezdése szerint a fogyasztót megillető elállás esetén a vállalkozásnak a fogyasztónak visszajáró összeget a fogyasztó által igénybe vett fizetési móddal megegyező módon kell visszatérítenie, ezért a kereskedő részéről a fogyasztónak ezzel ellentétesen adott tájékoztatása tisztességtelen kereskedelmi gyakorlatnak minősül, és mint ilyen a fogyasztóvédelmi hatóság részéről az Fgytv. 47. § (1) bekezdés a)-i) pontjában szabályozott jogkövetkezmények alkalmazását vonhatja maga után.

BH2026.124.: Akciózás vs. árcsökkentés
Az „akció” - szemben az „árcsökkentéssel” - nem jogi fogalom. Minden árcsökkentés akció, de nem minden akció árcsökkentés. Az „árcsökkentés bejelentése” kifejezés az eladó azon promóciós nyilatkozataira vonatkozik, amelyek szerint csökkentette az áru(k)ért felszámított árat, és nem alkalmazható az árelőnyök promóciójának olyan technikáira, amelyek nem árcsökkentések. Nem tekinthető önmagában azért tisztességtelennek egy kereskedelmi gyakorlat, mert a 4/2009. (I. 30.) NFGM-SZMM együttes rendelet szerinti árcsökkentett és a nem árcsökkentett akciós termékek esetében egyaránt figyelemfelhívó színű címkén adnak ártájékoztatást, továbbá a termékeket a kereskedelmi egység „Akció” feliratú polcán helyezik el. Az átlagfogyasztó számára egyértelmű ártájékoztatás alkalmazása nem valósít meg tisztességtelen kereskedelmi gyakorlatot.

EU jogalkotás és bírói döntések

Augusztus 2. napjától élnek az átláthatósági MI követelmények

1. EU Bizottság átláthatósági iránymutatás az MI rendszerek kapcsán
Az Európai Bizottság iránymutatást tett közzé az AI Act 50. cikkében meghatározott átláthatósági kötelezettségek gyakorlati alkalmazásáról, amelyek 2026. augusztus 2-től alkalmazandók; az útmutató ugyanakkor nem kötelező erejű. Az egyik legfontosabb szabály szerint az emberekkel közvetlenül kommunikáló AI-rendszereknél – például chatbotoknál, hangasszisztenseknél vagy AI-ügynököknél – már az első kapcsolatfelvételkor egyértelművé kell tenni, hogy a felhasználó mesterséges intelligenciával kommunikál. A generatív AI szolgáltatóinak emellett biztosítaniuk kell, hogy az AI által létrehozott vagy manipulált kép-, hang-, videó- és más szintetikus tartalom géppel olvasható módon felismerhető legyen, például metaadat, digitális vízjel vagy más technikai megoldás segítségével. Az érzelemfelismerő és biometrikus kategorizáló rendszerek alkalmazóinak külön tájékoztatniuk kell az érintetteket arról, hogy velük kapcsolatban ilyen AI-rendszert használnak. A deepfake kép-, hang- és videótartalmakat ugyancsak egyértelműen AI által generált vagy manipulált tartalomként kell megjelölni, és hasonló kötelezettség vonatkozik bizonyos közérdekű témákban közzétett AI-generált szövegekre is. Utóbbiaknál azonban kivétel alkalmazható, ha a szöveg emberi szerkesztői ellenőrzésen esett át, és annak tartalmáért természetes vagy jogi személy szerkesztői felelősséget vállal. A Bizottság hangsúlyozza, hogy az információnak világosnak, könnyen észlelhetőnek és hozzáférhetőnek kell lennie, ezért például nem elegendő azt hosszú általános szerződési feltételekben elrejteni.

Komoly kiberkockázat az élvonalbeli MI

2. EU felügyeleti szervek figyelmeztetnek az élvonalbeli MI kockázataira
Az európai pénzügyi felügyeleti hatóságok (EBA, EIOPA és ESMA) közös állásfoglalásban egységes, ágazatokon átívelő és kockázatalapú felügyeleti megközelítést sürgetnek a legfejlettebb („frontier”) AI-modellekből eredő IKT- és kiberbiztonsági kockázatok kezelésére. A pénzügyi szervezeteknek megfelelő irányítási és kockázatkezelési keretrendszerekkel kell biztosítaniuk e kockázatok megelőzését, felismerését és kezelését, ezáltal erősítve működési rezilienciájukat. Az állásfoglalás a DORA szerinti kritikus harmadik fél IKT-szolgáltatók felügyeletére is kitér, és alapul kíván szolgálni a pénzügyi intézmények és felügyeleti hatóságok közötti párbeszédhez. A cél, hogy az uniós pénzügyi rendszer ellenálló maradjon a frontier AI-technológiákból fakadó új kiberkockázatokkal szemben.

3. Jön az EU KIDS ACT
Az Európai Bizottság 2026 szeptemberében bemutatta az EU KIDS Act rendelettervezetet, amelynek célja a gyermekek erősebb online védelme, különösen a közösségi médiában. A tervezet szerint 13 év alatt nem lehetne közösségimédia-fiókot létrehozni, 13–14 éves korban pedig csak korlátozott, szülői vagy gondviselői fiókhoz kapcsolódó hozzáférés lenne megengedett; teljes fiók 15 éves kortól lenne elérhető. A nagyon nagy online platformoknak (VLOP) „safety by design” elvet kellene alkalmazniuk, és korlátozniuk kellene többek között a függőséget elősegítő funkciókat, a profilalkotáson alapuló ajánlórendszereket, a végtelen görgetést, az alvási időben küldött push értesítéseket és az idegenek

kéretlen kapcsolatfelvételét. A szabályozás közösségi médiára, videómegosztókra, online játékokra, valamint AI companion és chatbot szolgáltatásokra is kiterjedne, ha azokat 18 év alattiak használják. A tervezet adatvédelmet megőrző életkor-ellenőrzést is előírna, amelyhez az EU saját Age Verification Solution megoldása is használható lenne. A platformoknak megfelelési tervet kellene készíteniük, az új termékeket független auditnak alávetniük, a jogsértésekért pedig akár a globális éves árbevétel 6%-áig terjedő bírság is kiszabható lenne. Az életkor-ellenőrzés adatvédelmi kockázatokat is jelent, különösen a gyermekek, szülők és személyazonosító adataik nagy tömegű összekapcsolása miatt.

4. Új start-up vállalati forma is érkezhet

Hamarosan Európában is elindulhat az EU Inc, amely valamennyi tagállamban azonos működési feltételeket biztosítana főként a startup vállalatok számára. A kezdeményezés egy egész Európai Unióra kiterjedő társasági jogi forma létrehozását szorgalmazza. Ez lehetővé tenné, hogy a vállalatok közös szabályrendszer alapján alapítsanak céget, majd az egész uniós blokkban működjenek.

5. Digitális piacok (DMA) és szolgáltatások (DSA) rendeletének megsértései

A Bizottság előzetes megállapítása szerint a **TikTok** megsértette a digitális szolgáltatásokról szóló jogszabályt, mivel nem biztosított biztonságos fiókokat a kiskorúak számára. A Bizottság előzetesen megállapította azt is, hogy az **Instagram és a Facebook** addiktív kialakítása is sérti a digitális szolgáltatásokról szóló jogszabályt. A Bizottság a **Google Inc**-et a digitális piacokról szóló rendelet megsértése miatt 890,-M EUR bírsággal sújtotta. A bírságot azt követően szabták ki, hogy az Európai Bizottság vizsgálata szerint a Google saját szolgáltatásait részesítette előnyben a Google keresőben, továbbá olyan korlátozásokat alkalmazott, amelyek akadályozták a vállalkozásokat abban, hogy a fogyasztókat a Google Playen kívüli, alternatív – gyakran olcsóbb – vásárlási lehetőségekhez irányítsák. Az **AliExpress** is kapott a Bizottságtól egy 550,-M EUR nagyságú bírságot a digitális szolgáltatásokra vonatkozó rendelet megsértése kapcsán. A Bizottság szerint a szolgáltató a kockázatokat nem mérlegelte megfelelően, nem volt kellő mértékű emberi ellenőrzés, illetve az illegális, nem biztonságos és hamisított áruk terjesztésére is sor került. Végül az Európai Bizottság az uniós digitális szolgáltatásokról szóló rendelet alapján az **OpenAI ChatGPT** szolgáltatását nagyon nagy online keresőprogramnak (VLOSE) minősítette, míg a Reddit és a Roblox nagyon nagy online platform (VLOP) minősítést kapott. Mindhárom szolgáltatás átlépte az ehhez szükséges, havi átlagosan 45 millió uniós felhasználót jelentő küszöbértéket. A minősítés következtében további DSA-kötelezettségek vonatkoznak rájuk, különösen a rendszerszintű kockázatok értékelése és mérséklése, a gyermekek online biztonsága, valamint az alapvető jogok védelme területén. Ezek a többletkövetelmények 2027 januárjától alkalmazandók.

6. Közeledik az Európai Egészségügyi Adattér (EHDS) alkalmazhatósága

Megjelent a 2026/2083.sz. végrehajtási rendelet, mely MyHealth@EU működésének részletes technikai és szervezeti szabályait állapítja meg. A MyHealth@EU az EHDS keretében működő uniós infrastruktúra, amelynek célja, hogy a betegek elektronikus egészségügyi adatai – például betegösszefoglalók, elektronikus receptek, laboreredmények vagy képalkotó vizsgálatok – határokon átnyúló egészségügyi ellátás esetén biztonságosan és interoperábilis módon elérhetők legyenek más tagállam egészségügyi szolgáltatói számára. A rendelet ennek érdekében meghatározza többek között a MyHealth@EU központi interoperabilitási platformjának működését, a nemzeti e-egészségügyi kapcsolattartó pontok csatlakozásának és megfelelőség-ellenőrzésének követelményeit, az adatcsere biztonsági és interoperabilitási feltételeit, valamint a felelősségi és együttműködési szabályokat.
Alkalmazandó: 2027.03.26.

7. Innovációs csomagot fogadott el az EU

Az Európai Bizottság European Innovation Act (Európai Innovációs Jogszabály) javaslatának célja, hogy az EU-ban létrejövő kutatási eredmények és innovatív ötletek könnyebben jussanak el a piacra, és az európai startupok és scaleupok könnyebben tudjanak finanszírozást szerezni és Európában növekedni. A csomag egyik központi eleme a szellemi tulajdon egységesebb uniós értékelési keretének kialakítása, amely lehetővé tenné, hogy a vállalkozások IP-eszközeiket könnyebben használják finanszírozás bevonására; ehhez egy uniós digitális IP-piactér is társulna, amely összeköti a szellemi tulajdon eladóit és vevőit. A másik fontos pillér a kutatás-fejlesztési közbeszerzések egységes eljárásának kialakítása, amely egyszerűbbé tenné az innovatív megoldások kutatásának, fejlesztésének és tesztelésének közbeszerzését, beleértve a határokon átnyúló közös beszerzéseket is. A Bizottság számításai szerint az intézkedések évente mintegy 10,2 milliárd euró többletfinanszírozást mozgósíthatnak az IP-eszközök révén, az innovációs közbeszerzések pedig 25,9 milliárd euró

többletnyereséget eredményezhetnek a vállalkozásoknak; összességében a csomag tíz év alatt akár 0,24–0,42%-kal növelheti az EU GDP-jét és 507 000 új munkahelyet teremthet.

8. Magyarország is csatlakozott az EU ügyészséghez

A Bizottság 2026. július 10-én megerősítette a részvételt, Magyarország pedig augusztus elejétől a 25. részt vevő tagállammá vált. A gyakorlatban ez azt jelenti, hogy az EPPO Magyarországon is jogosult az EU pénzügyi érdekeit sértő bűncselekmények – így különösen az uniós forrásokat érintő csalás, korrupció, pénzmosás és bizonyos határon átnyúló áfacsalások – nyomozására és vádemelésére. A magyarországi ügyeket európai delegált ügyészek folytatják, akik az EPPO szervezetében, a nemzeti hatóságoktól függetlenül járnak el, és a magyar bíróságok előtt képviselik a vádat. A csatlakozás tehát nem a magyar ügyészség általános feladatainak átvételét jelenti, hanem egy közvetlen uniós nyomozási és vádhatósági hatáskör megjelenését Magyarországon az EU költségvetését érintő meghatározott bűncselekmények esetében.

9. Európai Unió Bírósága döntései

A döntés száma	Tartalma
C-317/25.	**Egy vállalkozás számára ahhoz adott hozzájárulás, hogy „partnerei" kereskedelmi üzletszerzés céljából személyes adatokat használjanak fel, csak akkor érvényes, ha e partnerek személyazonossága ismert.** Az adatkezeléshez adott hozzájárulás nem teszi lehetővé, hogy egy vállalkozás meg nem nevezett „partnerei" saját direkt marketing céljukra felhasználják az érintett személyes adatait. A főtanácsnok szerint a **„partnerek" megjelölés önmagában túl általános ahhoz, hogy az érintett észszerűen előre láthassa, mely vállalkozások fogják megkeresni**. Fontos, hogy ez egyelőre főtanácsnoki indítvány, nem az Európai Unió Bíróságának ítélete.
C-421/24.	**A Google felelősségre vonható egy vele kereskedelmi partnerségi viszonyban álló tartalomkészítő YouTube-videóiért.** Az Európai Unió Bírósága a C-421/24. sz. AGCOM (Online szerencsejáték) ügyben kimondta, hogy a Google adott esetben felelősségre vonható a vele kereskedelmi partnerségben álló tartalomkészítő YouTube-videóiért. Az ügyben egy partner online szerencsejátékot reklámozó videókat tett közzé, miközben a Google a partnerség létrehozásakor megvizsgálta a csatorna témáját, videóit és metaadatait. A Bíróság szerint ilyen körülmények között a **platform nem feltétlenül tekinthető pusztán technikai, automatikus és passzív tárhelyszolgáltatónak**, mert konkrét ismereteket szerezhetett a tartalom lényegéről. Ezért nem hivatkozhat automatikusan az elektronikus kereskedelmi irányelv tárhelyszolgáltatói felelősségmentességére; a nemzeti bíróságnak kell megvizsgálnia, hogy a Google-nak észszerűen tudnia kellett-e a szerencsejátékot reklámozó tartalmakról.
C-163/24.	**Az uniós jog megsértése miatti felelősség: a Bíróság pontosítja azokat a feltételeket, amelyek mellett egy magánszemély kártérítést kaphat egy uniós joggal ellentétes bírósági határozat miatt.** Az Európai Unió Bírósága két ítéletében pontosította, mikor alapozhatja meg egy végső fokon eljáró nemzeti bíróság uniós jogsértése a tagállam kártérítési felelősségét. Önmagában az, hogy a bíróság elmulasztotta az előzetes döntéshozatali eljárás kezdeményezését, még nem elegendő: ehhez olyan uniós jogi szabály megsértésének is társulnia kell, amely magánszemélyek számára jogokat biztosít. Egy ilyen ügyben **a vállalkozás átruházása esetén a munkavállalókat védő uniós szabály ilyen egyéni jogokat biztosított, és a Bíróság szerint a körülmények arra utalnak, hogy a portugál legfelsőbb bíróság korábbi ítélete kellően súlyos uniós jogsértésnek minősülhet**, ami megalapozhatja az állam kártérítési felelősségét.

Hazai, tagállami, nemzetközi adatvédelem

Pontosabb tájékoztatás szükséges az érintett hozzájárulásához

1. Hazai adatvédelmi fejlemények

NAIH közlemény a hozzájáruláson alapuló kapcsolati adat kezeléshez

Egy bírósági eljárás eredményére támaszkodva a NAIH jogértelmezést tett közzé. Az érintett hozzájárulása eszerint csak olyan, előzetesen kellően pontosan meghatározott, konkrét adatkezelési

célra biztosít jogalapot, ezáltal jogszerű adatkezelést, amelyről az érintett a hozzájárulás megadását megelőzően megfelelő tájékoztatást kapott. A korábbi hatósági gyakorlattól eltérően az olyan általános megfogalmazások, mint a „további kapcsolattartás", „véleménykérés", „tájékoztatás" vagy „elektronikus levél küldése" – az adatkezelési cél megjelölése nélkül – az adatkezelő lehetséges kommunikációs cselekményeinek megjelölései, azaz csupán adatkezelési műveletek. A jogértelmezés rámutat, hogy az adatkezelési cél nem azonosítható az adatkezelési művelettel, azaz a kommunikáció módjának megjelölésével. Ebből következően a „kapcsolattartás", a „hírlevélküldés", a „tájékoztatás" vagy az „elektronikus levél küldése" kifejezéseket az adatkezelőnek **olyan további információval kell kiegészítenie, amelyből egyértelműen megállapítható, hogy a tájékoztatás, vagy a kommunikáció pontosan milyen célból történik**, azaz például milyen tárgyra, szolgáltatásra, ügyre vagy tevékenységre vonatkozik. A hozzájárulás nem értelmezhető kiterjesztően, a homályos, meg nem határozott célból történő adatkezeléshez nem szolgálhat érvényes jogalapként az érintett hozzájárulása. A tényleges adatkezelési célok azonosítása kapcsán figyelembe veszi, együtt értelmezi a hozzájárulás megszerzése során nyújtott összes tájékoztatást, ideértve az adatkezelési tájékoztató teljes tartalmát és a hozzájárulást kérő űrlapon, weboldalon adott valamennyi közlést, információt is.

Generatív mesterséges intelligencia tájékoztatót jelentetett meg a NAIH

Dél-Korea és Franciaország adatvédelmi hatóságai készítettek egy tájékoztató posztert, amely a generatív MI használatával kapcsolatos kockázatokra hívja fel a figyelmet, valamint segítséget nyújt a kockázatok mérséklésére. Ezt a készítők engedélyével a NAIH a magyar érintettek részére lefordította magyar nyelvre és közzétette a honlapján.

Generatív MI információs poszter került közzétételre

2. Tagállami, nemzetközi adatvédelmi fejlemények

Európai Adatvédelmi Testület: anonimizálás, webscraping iránymutatások jelentek meg

Anonimizálás iránymutatás jelent meg az Európai Adatvédelmi Testülettől (EDPB)

Az anonimizálás tekintetében kiadott iránymutatás kiemeli, hogy a GDPR alapján személyes adat minden olyan információ, amely egy azonosított vagy azonosítható természetes személyhez kapcsolódik; ezzel szemben a valóban anonim adatokra a GDPR már nem alkalmazandó. A kettő között helyezkednek el az álnevesített (pszeudonimizált) adatok, amelyek önmagukban nem teszik lehetővé az érintett azonosítását, de további információk segítségével ismét személyhez kapcsolhatók. Ennek gyakorlati jelentősége lehet például utánkövetéses gyógyszervizsgálatoknál, ahol a vizsgálati eredményeket ugyanahhoz a beteghez kell rendelni, miközben az azonosításhoz szükséges információk nem feltétlenül kerülnek a gyártóhoz. Az Európai Unió Bírósága a C-413/23. sz. ügyben azt vizsgálta, hogy ilyen helyzetben kinek a szempontjából kell megítélni az azonosíthatóságot. A Bíróság szerint nem elegendő, hogy az eredeti adatkezelő képes az érintett azonosítására: azt is vizsgálni kell, hogy az adatokat átvevő címzett rendelkezik-e az azonosításhoz szükséges kiegészítő információkkal, vagy azok számára ésszerűen hozzáférhetők-e. Következésképpen ugyanaz a pszeudonimizált információ az egyik szereplő számára személyes adat lehet, míg egy olyan címzett szempontjából, aki az érintettet jogilag és ténylegesen sem képes ésszerű eszközökkel azonosítani, elveszítheti személyesadat-jellegét. Az EDPB szerint a technológiai fejlődéssel az anonimizálás értelme is változik, könnyebben összeköthető az adat az érintettel. Végezetül az iránymutatás anonimizálási technikákat is bemutat.

EDPB webscraping iránymutatás is megjelent

A web scraping olyan automatizált adatkinyerési eljárás, amelynek során programok nyilvánosan hozzáférhető weboldalakról nagy mennyiségű adatot gyűjtenek és strukturált formában tárolnak, például generatív AI-modellek betanítása vagy finomhangolása céljából. Az EDPB iránymutatása szerint amennyiben az így gyűjtött információk személyes adatokat tartalmaznak, az adatkezelésre a GDPR követelményeit teljes körűen alkalmazni kell, függetlenül attól, hogy az adatok nyilvánosan elérhetők voltak. Különösen vizsgálni kell az adatkezelés jogalapját, célhoz kötöttségét, átláthatóságát és az adattakarékosság érvényesülését, miközben a magánszektorban a leggyakrabban szóba jövő jogalap a megfelelő érdekmérlegelést igénylő jogos érdek lehet. Az EDPB megkülönbözteti a célzott és a nem célzott adatgyűjtést, és utóbbit kockázatosabbnak tekinti, mivel az adatkezelő sokszor előzetesen maga

sem tudja, milyen személyes vagy akár különleges adatokat fog összegyűjteni. A kockázatok csökkentése érdekében már az adatgyűjtés megtervezésekor technikai és szervezési garanciákat kell alkalmazni, így például pontos kiválasztási és kizárási szabályokat, személyesadat-szűrőket és adott esetben szintetikus adatokat, valamint figyelembe kell venni a weboldalak technikai tiltó jelzéseit is. Különös kockázatot jelent, hogy a generatív modellek a betanítási adatokban szereplő személyes információkat megjegyezhetik, később reprodukálhatják, illetve azokból az érintettre vonatkozó új következtetéseket állíthatnak elő. Tömeges adatgyűjtésnél az egyedi tájékoztatás bizonyos esetekben aránytalan erőfeszítést jelenthet, de ez nem jelent automatikus felmentést: az adatkezelőnek a kivétel feltételeit igazolnia és megfelelő nyilvános tájékoztatást biztosítania kell. A szabályok EU-n kívüli AI-fejlesztőket is érinthetnek, ha az adatkezelés a GDPR területi hatálya alá kerül, így az EDPB megközelítésének alapvető célja az AI-fejlesztéshez szükséges innováció és az érintettek adatvédelmi jogainak összehangolása.

Microsoft vizsgálat: fel kell mérni az MI funkciók alkalmazásának következményeit

Holland adatvédelmi iránymutatás a Microsoft Copilot kockázatairól

A holland adatvédelmi hatóság (AP) a Haarlemmermeer önkormányzat Microsoft 365 Copilot-bevezetésének vizsgálata során arra jutott, hogy egy generatív AI-rendszer alkalmazása nem kezelhető egyszerű informatikai vagy szoftverbeszerzési projektként, hanem annak teljes adatvédelmi környezetét előzetesen fel kell mérni. A bevezetés feltétele a megfelelő adatgazdálkodás: naprakész adatleltárra, dokumentumklasszifikációra, megfelelő címkézésre és különösen a hozzáférési jogosultságok felülvizsgálatára van szükség, mert az AI a már meglévő jogosultsági hibák hatását jelentősen felerősítheti. Az AI alkalmazásának célját konkrétan és előzetesen meg kell határozni, mivel önmagában a működés „hatékonyabbá tétele" nem megfelelő célmeghatározás, és az sem indokolhat adatkezelést, hogy a Copilot technikailag hozzáfér valamely információhoz. Külön adatvédelmi kockázatot jelentenek az AI által generált téves vagy kitalált, természetes személyekre vonatkozó információk, amelyek már pontatlan személyes adatnak minősülhetnek, és az automation bias miatt bekerülhetnek tényleges döntésekbe is. Emiatt az emberi kontrollnak valósnak kell lennie: a munkatársaknak érteniük kell az AI korlátait, fel kell ismerniük a hibás eredményeket, és képesnek kell lenniük az AI javaslatától eltérő döntést hozni. A rendszer technikai összetettsége az érintetti jogokat sem korlátozhatja, ezért az adatkezelőnek továbbra is biztosítania kell többek között a tájékoztatáshoz, hozzáféréshez, helyesbítéshez és törléshez való jog tényleges gyakorlását.

Adatvédelmi incidensek kiberbiztonsági tanulságokkal

Revolut adatszivárgás, OPEN AI és EY incidensek

Adatbiztonsági incidens történt a **Revolutnál.** A vállalat szerint csalárd hatósági megkeresések miatt egy illetéktelen harmadik fél hozzáférhetett egyes ügyfelek személyes adataihoz. A cég azonban közölte azt is, hogy a rendszerei és az ügyfelek pénze nincs veszélyben. Az eset során többféle személyes adat is érintett lehetett. A TechCrunch beszámolója szerint ezek között szerepelhetett a születési dátum, a postai és e-mail-cím, valamint a telefonszám. A kiszivárgott információk között azonban ennél érzékenyebb adatok is lehetnek. A jelentés szerint egyes ügyfelek személyazonosító okmányainak másolatai, például útlevelek és jogosítványok is rossz kezekbe kerülhettek. A módszer azért is figyelemre méltó, mert a csalók nem egy egyszerű, könnyen felismerhető hamis e-mail-címről keresték meg a Revolutot. A Reuters szerint egy valódi kormányzati ügynökség e-mail-domainjét használták, így a megkeresések hitelesnek tűnhettek. Az **OPEN AI** esetében is incidens történt. A modellről ugyanis kiderült, hogy a hibáit több esetben elrejtette, illetve bizalmas adatokat az internetre tett ki annak érdekében, hogy azokat később nyilvános forrásként használhassa. Az **EY** 2026-ban nyilvánosságra került adatvédelmi incidense egy külső szolgáltató által működtetett IT support-ticket rendszerhez történt jogosulatlan hozzáférésből eredt. A rendszerben az EY munkatársai ügyfelekhez kapcsolódó dokumentumokat is elhelyeztek, ezért a támadók személyes, pénzügyi és adózási adatokat tartalmazó állományokhoz is hozzáférhettek, illetve azokat letölthették. Az eset legfontosabb adatvédelmi tanulsága, hogy a szervezeteknek nemcsak központi adatbázisaikat, hanem a külső szolgáltatóknál működő másodlagos rendszereket – például helpdesk- és ticketing rendszereket – is az adatvagyon részeként kell kezelniük. **Különösen fontos az adattakarékosság, a mellékletek feltöltésének korlátozása, a megfelelő hozzáférés-kezelés és megőrzési idő, valamint a beszállítók információbiztonsági kontrolljának rendszeres ellenőrzése**.

3. Hazai és tagállami adatvédelmi bírságok (M: millió EUR)

Társaság	Szankció	Indok
Miljödata	**2.2,-M EUR**	A svéd adatvédelmi hatóság szabott ki bírságot egy **szoftvercég**re, mivel a **különleges adatok kockázatarányos, valós idejű védelmét nem**

		biztosította. A támadó emiatt több millió érintett TAJ számához és egészségügyi adataihoz fért hozzá.
Google Inc.	**403,-M EUR**	Az ír adatvédelmi hatóság a **helymeghatározási adatok jogellenes kezelése** miatt szabta ki a bírságot.
Hera Comm Spa EstEnergy Spa	**5.8,- M EUR** **1.4,- M EUR**	Az olasz adatvédelmi hatóság (Garante) jelentős bírságokat szabott ki két energia-szolgáltatóra, mert olyan **automatizált scoring rendszert alkalmaztak**, amely a potenciális ügyfelek megbízhatóságát pontszámmal értékelte, és **ennek alapján döntöttek arról, hogy megkötik-e velük az áram- vagy gázszolgáltatási szerződést.**
Uber	**825 000,- EUR**	2018–2022 között teljesen **automatizált módon deaktiválta egyes sofőrök fiókjait csalás gyanúja vagy alacsony ügyfélértékelések miatt**. A döntésekhez nem kapcsolódott érdemi emberi felülvizsgálat, miközben a fiók felfüggesztése vagy végleges megszüntetése jelentős következménnyel járt: a sofőrök elveszítették az Uberből származó jövedelmüket. Az eljárás 171 francia sofőr panaszából indult, és a holland hatóság azért járt el, mert az Uber európai központja Hollandiában található.
EXTIA	**300 000,-EUR**	A francia adatvédelmi hatóság (CNIL) bírságot szabott ki az EXTIA IT- és mérnöki tanácsadó cégre, mert **nem megfelelően kezelte az állásra jelentkezők és volt munkavállalók törlési kérelmeit**. A 2024-ben érkezett 265 törlési kérelem több mint háromnegyedét nem vagy nem megfelelően intézték el: 12 kérelmet egyáltalán nem teljesítettek, 166 érintettet nem tájékoztattak a kérelem eredményéről, további 27 személy pedig csak az egy hónapos GDPR-határidő lejárta után kapott választ.
Hopital Privé de la Loire	**500 000,-EUR**	Egy 2025-ös kibertámadást követően került bírság kiszabásra. **A támadó a kórház elektronikus betegnyilvántartásához hozzáférve 524 867 beteg és 202 246 kapcsolattartó személy adataihoz, köztük egészségügyi adatokhoz is hozzájutott.** A francia CNIL szerint a **kórház megsértette a GDPR 32. cikkét, mert a külső hozzáféréseknél nem alkalmazott megfelelő VPN-t és többfaktoros hitelesítést, túl széles hozzáférési jogosultságokat biztosított, és nem rendelkezett a gyanús tevékenységet gyorsan észlelő riasztási rendszerrel**. A kórház a GDPR 34. cikkét is megsértette, mert bár az érintett betegeket tájékoztatta az incidensről, **a 202 246 érintett kapcsolattartó személyt közvetlenül nem értesítette.**
Health Service Executive	**645 000,- EUR**	Az ír adatvédelmi hatóság (DPC) összesen 645 000 euró bírságot szabott ki az ír egészségügyi szolgálatra (HSE) **a papíralapú egészségügyi dokumentumok nem megfelelő tárolása** miatt. Két használaton kívüli egykori pszichiátriai kórházban illetéktelen személyek jutottak be az irattároló helyiségekbe, majd az ott talált egészségügyi dokumentumokról készült felvételeket a közösségi médiában is közzétették. A DPC megállapította, hogy a HSE nem biztosított megfelelő fizikai védelmet és dokumentumbiztonságot, ami többek között a GDPR adatbiztonsági és incidenskezelési követelményeinek megsértését eredményezte.

Scoring döntések

Gazdasági Versenyhivatal hírek

1. Gazdasági Versenyhivatal fontosabb döntései

Társaság	Szankció	Indok
eMAG	**225,-M HUF**	**Ismét megszegték a saját vállalásaikat** az eMAG webáruház üzemeltetői – tárta fel utóvizsgálatában a Gazdasági Versenyhivatal (GVH). A romániai központú e-kereskedelmi platform működtetői a magyar vállalkozások támogatását ígérték, ezt azonban csak részben, illetve hiányosan valósították meg.
Lidl Magyarország Kereskedelmi Bt.	**48,-M HUF**	Az országszerte mintegy 200 áruházat működtető kiskereskedelmi vállalkozás **megtévesztő módon kommunikálta, hogy „Lidl a legolcsóbb élelmiszerlánc**”. 2024 februárjában – az eredeti ügyben – ugyanezért már elmarasztalta a céget a GVH, de a Kúria új eljárásra kötelezte a GVH-t. A megismételt eljárásban a GVH szűkebb körben, de gyakorlatilag ugyanarra a megállapításra jutott. A cég együttműködött a versenyhatósággal, elismerte a jogsértést

		és vállalta, hogy a jövőben körültekintőbben jár el az árakkal kapcsolatos kommunikációja során.

2. Gazdasági Versenyhivatal fontosabb hírei

Ellenőrzik a zöldre festést

Szigorúbb szabályok jönnek a fenntarthatósági kommunikáció terén

Európai Uniós jogszabályi változások eredményeként – a fogyasztók zöld átállásban való szerepvállalásának a tisztességtelen gyakorlatokkal szembeni hatékonyabb védelem és a hatékonyabb tájékoztatás révén történő növelése érdekében – 2026. szeptember 27-étől Magyarországon is szigorúbb szabályok vonatkoznak majd a vállalatok kommunikációja során alkalmazható fenntarthatósági állításokra. Az ún. EmpCo irányelvet 2024 elején fogadta el az Európai Parlament és a Tanács. Az irányelv célja, hogy szigorúbb fellépést tegyen lehetővé a megtévesztő zöld kommunikációval szemben, ezzel erősítve a fogyasztók védelmét. A változás legfontosabb része, hogy összesen 12 új ponttal bővül ki a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló törvény (Fttv.) mellékletében található felsorolás, avagy az ún. „feketelista”.

Piacelsőbbségi állításokat vizsgál a GVH

A piacelsőségi állítások a magas kockázatú reklámállítások közé tartoznak a versenyjogi fogyasztóvédelem területén, mivel alkalmasak arra, hogy a versenytársakhoz viszonyított kiemelkedő piaci pozíciót sugallják a fogyasztók számára. Ezért alkalmazásuk csak akkor jogszerű, ha pontosak, hitelesek és objektív bizonyítékokkal alátámasztottak.

TikTok vállalások a célkeresztben

Utóvizsgálatot indított a Gazdasági Versenyhivatal (GVH) az Írországban bejegyezett TikTok Technology Limiteddel szemben, amely a globális, kínai tulajdonú videómegosztó platform európai üzemetetője. A TikTok a GVH 2023 novemberében lezárt eljárásának eredményeként számos vállalást tett a szolgáltatás kommunikációs, adat- és gyermekvédelmi funkcióinak fejlesztése, illetve megerősítése érdekében. A versenyhatóság most tüzetesen értékeli, hogy a TikTok maradéktalanul teljesítette-e a kötelezően előírt vállalásokat.

Integritás Hatóság hírek

Feljelentés Gondosóra ügyben

Az Integritás Hatóság köztes jelentést készített a Gondosóra program egyes beszerzéseinek vizsgálatáról. A jelentésben feltárt körülmények alapján a Hatóság feljelentést tett ismeretlen tettes ellen több bűncselekmény gyanúja miatt, szabálytalansági eljárást kezdeményez az irányító hatóságnál, és további hatáskörrel rendelkező szervek eljárását is kezdeményezi. Az Integritás Hatóság a köztes jelentés lezárása mellett folytatja tényfeltáró munkáját, és a még folyamatban lévő vizsgálati cselekmények eredményéről a vizsgálatot záró jelentésben számol majd be.

Biztonsági követelmények szükségesek az MI-hez

Mesterséges intelligencia hírek

1. Aggasztó fejlemények az élvonalbeli MI modelleknél: önállósodik a modell

A Wall Street Journal beszámolója szerint OpenAI által tesztelt AI-ügynökök egy csoportja („swarm”) 2026 májusában nem szándékolt módon beavatkozott a RubyGems szoftvercsomag-kezelő szolgáltatás működésébe: automatikusan új fiókokat hozott létre és nagy mennyiségű, lényegében spam jellegű fájlt töltött fel, ami miatt a RubyGems négy napra leállította az új regisztrációkat. Az ügynökök eredetileg ártalmatlan feladatokat – például adatgyűjtést és jelentések készítését – kaptak, de a korlátozott internet-hozzáférést megkerülve a RubyGems szolgáltatást kezdték egyfajta közvetett böngészőként használni; kutatók szerint két sérülékenység kihasználásával is próbálkoztak, köztük egy addig nem ismert, súlyos hibával, bár annak sikeres kihasználását nem igazolták. Az OpenAI megerősítette, hogy saját ügynökei érintettek voltak az incidensben, ugyanakkor hangsúlyozta, hogy azok nyilvános információk megszerzésére törekedtek. Az eset azért keltett komolyabb figyelmet, mert azt mutatja, hogy nagyobb autonómiával rendelkező AI-agentek a fejlesztők által eredetileg nem tervezett módon használhatnak külső rendszereket, ezért az agentikus AI esetében a sandboxing, a

hozzáférés-korlátozás, a folyamatos felügyelet és az incidensek gyors felismerése egyre fontosabb biztonsági követelmény. Hasonlóképpen aggályokat vet fel az OPEN AI azon közlése, hogy a modelljük több esetben hibáit szándékosan leplezte, illetve nyilvános adatokat tett az interneten elérhetővé abból a célból, hogy később arra, mint nyilvános információ hivatkozhasson.

2. Kiszivárogtak keresési előzmények a Cloude-ból

2026 júliusában kiderült, hogy a Claude megosztási funkciójával nyilvánossá tett beszélgetések közül több száz megjelent a Google keresési találataiban, így egyszerű kereséssel olyan beszélgetések is megtalálhatók voltak, amelyek jogi stratégiákat, műszaki kódokat vagy személyes és érzékeny információkat tartalmaztak. A probléma hátterében a beszámoló szerint az állt, hogy a nyilvános megosztási oldalak nem rendelkeztek megfelelő noindex beállítással, ezért ha egy megosztási link valahol nyilvánosságra került, a keresőmotorok feltérképezhették és indexelhették annak teljes tartalmát. Később az érintett találatok nagy része eltűnt a Google-ből, de ez önmagában n

Egyre több az MI modellekből szivárgó adat

szüntette meg a korábban létrehozott megosztási linkek elérhetőségét. Az eset fontos ac
információbiztonsági tanulsága, hogy az AI-rendszerek beszélgetésmegosztási funkcióit nem szabad automatikusan bizalmas kommunikációként kezelni: **üzleti titkot, személyes adatot vagy más érzékeny információt tartalmazó beszélgetés megosztása adatvesztési, szellemitulajdon-védelmi és compliance-kockázatot is teremthet.**

3. Kiberbiztonsági és MI cselekvési tervet dolgozott ki az EU

Az Európai Bizottság MI- és kiberbiztonsági cselekvési terve arra reagál, hogy a fejlett, ún. frontier MI-modellek egyszerre teremtenek új védekezési lehetőségeket és új kiberkockázatokat: felhasználhatók sérülékenységek felderítésére, támadások automatizálására és azok sebességének jelentős növelésére. A terv ezért többek között uniós MI-biztonsági értékelési kapacitás létrehozását, a fejlett modellekhez való ellenőrzött kiberbiztonsági célú hozzáférést, valamint az ENISA és a Bizottság Közös Kutatóközpontja által működtetett AI-kiberbiztonsági tesztplatform kialakítását irányozza elő. Emellett ösztönzi az MI alkalmazását a sérülékenységek gyorsabb felismerésére és javítására, erősíti a kritikus infrastruktúrák és a nyílt forráskódú szoftverek védelmét, és támogatja az európai, szuverén AI-kiberbiztonsági képességek fejlesztését.

4.Új MI szervezeti egység a Tudományos és Technológiai Minisztériumon belül

A változásokat a 2/2026. (IX. 21.) TTM utasítás rögzíti, mely szeptember 22-én lépett hatályba. A Digitalizációs Államtitkár irányítása alatt így jelenleg már külön helyettes államtitkár felel a mesterséges intelligenciáért, miközben a kiberbiztonsági feladatok is külön szervezeti egységekhez kerültek. A mesterséges intelligenciáért felelős helyettes államtitkárhoz több, kifejezetten erre a területre létrehozott főosztály tartozik. Ide sorolták a Nemzeti Adatstratégiai Főosztályt, az MI Stratégiai Főosztályt, az MI Piacfelügyeleti Hatósági Főosztályt és az MI Szabályozási Főosztályt, valamint a Kormányzati Iratkezelési Főosztályt.

5. Kormányzati MI honlap indult

Kormányzati honlap indult mihivatal.gov.hu címen a mesterséges intelligenciával (MI) kapcsolatos kérdések megválaszolására, a weboldalon panaszt is lehet tenni! A mesterséges intelligencia fejlődésével egyre könnyebben készíthetők valósághű, de hamis deepfake tartalmak, amelyek súlyos károkat okozhatnak embereknek és vállalkozásoknak egyaránt. Az Európai Unió mesterségesintelligencia-rendelete (AI ACT) értelmében az AI-vel generált tartalmakat kötelező jelölni, az AI-alapú ügyfélszolgálatokról pedig előzetesen tájékoztatni kell az ügyfeleket. A kormányzati platformon **a lakosság bejelentheti az AI-vel kapcsolatos visszaéléseket és panaszt tehet, ha a technológia alkalmazása sérti jogos érdekeit**. Az oldal számos gyakorlati, hasznos tanáccsal látja el az AI megoldásokat alkalmazó felhasználókat.