EURÓPAI
BIZOTTSÁG

Brüsszel, 2025.12.11.
COM(2025) 752 final

A BIZOTTSÁG JELENTÉSE AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

amelyben az (EU) 2016/794 rendelet 68. cikke (3) bekezdésének megfelelően értékeli és felméri az (EU) 2022/991 rendeletben, különösen a 4. cikk (1) bekezdésének t) pontjában, a 18. cikk (2) bekezdésének e) pontjában, a 18. cikk (6a) bekezdésében, valamint a 18a., a 26., a 26a. és a 26b. cikkben az Europol célkitűzései tekintetében előírt feladatok végrehajtásának operatív hatását, valamint az említett feladatoknak a Chartában foglalt alapvető jogokra és szabadságokra gyakorolt hatását

{SWD(2025) 404 final}

1. Az értékelés köre

A Bűnüldözési Együttműködés Európai Uniós Ügynöksége (Europol) 1999-es megalakulása óta **központi szerepet játszik a határokon átnyúló súlyos bűnözés és a terrorizmus elleni küzdelemben**, és az európai bűnüldözési együttműködés egyik fő mozgatórugójává vált. A biztonsági helyzet az elmúlt 30 évben drasztikus változásokon ment keresztül, ami a súlyos és szervezett bűnözés jellegében („DNS"-ében) is változásokat eredményezett[1]. A tagállamoknak új operatív igényeik vannak a felmerülő fenyegetések hatékony kezelése terén, és **az Europol támogatásával kapcsolatos elvárásaik** is **megváltoztak**. Az Europol megbízatását ezért többször felváltották vagy módosították az Ügynökség relevanciájának fenntartása és fokozása érdekében.

Az Europolnak az (EU) 2016/794 rendeletben[2] (a továbbiakban: Europol-rendelet) meghatározott megbízatását legutóbb 2022-ben módosították az (EU) 2022/991 rendelettel[3] az új biztonsági fenyegetések kezelése érdekében. Az Europol-rendelet már nem felelt meg a célnak az új valóságban, amelyben a bűnözők kihasználják **a digitális átalakulás**, **az új technológiák**, **a globalizáció** és **a mobilitás** előnyeit[4].

Az (EU) 2022/991 rendelet[5] **konkrét célkitűzései** a következők voltak:

- hatékony együttműködés lehetővé tétele a **magánszereplők** és a bűnüldöző hatóságok között a bűnözők által a határokon átnyúló szolgáltatások kihasználásával elkövetett visszaélések elleni küzdelem érdekében,
- annak lehetővé tétele, hogy a bűnüldöző hatóságok az **alapvető jogok** teljes tiszteletben tartása mellett **nagy és összetett adatkészleteket** tudjanak elemezni a határokon átnyúló kapcsolatok felderítése érdekében,
- annak lehetővé tétele, hogy a tagállamok **új technológiákat** alkalmazzanak a bűnüldözés területén.

Emellett az (EU) 2022/991 rendelet a **magas szintű adatvédelem** fenntartása érdekében módosította az Europolra alkalmazandó adatvédelmi szabályokat, egyensúlyt teremtve az Ügynökségnek a személyes adatok kezelésére vonatkozó új hatásköre, valamint az egyének magánéletének és személyes adatainak védelme között. **Az információáramlás megkönnyítése érdekében** nagymértékben összehangolta az Europolra alkalmazandó adatvédelmi szabályokat az (EU) 2018/1875 rendelet (a továbbiakban: európai uniós adatvédelmi rendelet) IX. fejezete értelmében az egyéb uniós bel- és igazságügyi ügynökségekre és szervekre alkalmazandó adatvédelmi szabályokkal, valamint az (EU) 2016/680 irányelvet (a továbbiakban: a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv)[6] átültető, nemzeti joguk értelmében a tagállamok bűnüldöző hatóságaira (a továbbiakban: illetékes hatóságok) alkalmazandó szabályokkal.

---

1 Europol, 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) – The change DNA of serious and organised crime (Az Európai Unió súlyos és szervezett bűnözés általi fenyegetettségének 2025. évi értékelése [SOCTA]: A súlyos és szervezett bűnözés „DNS"-ének változása), online elérhető a következő címen: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf („EU SOCTA 2025"). Lásd még: Customs threat assessment (CTA) 2025 (2025. évi vámügyi fenyegetésértékelés [CTA]), online elérhető a következő címen: https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 HL L 135., 2016.5.24., 53. o., ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 HL L 169., 2022.6.27., 1. o., ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final, 2020. december 9., 37. o., https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Ugyanott.*

6 HL L 119., 2016.5.4., 89. o., ELI: http://data.europa.eu/eli/dir/2016/680/oj.

Ezt a jelentést a Bizottságnak **az Europol-rendelet 68. cikkének (3) bekezdésében** előírt kötelezettségével összhangban fogadták el, amely szerint három évvel a rendelet hatálybalépését követően értékelnie kell[7] és fel kell mérnie az Europolnak az (EU) 2022/991 rendeletben meghatározott feladatainak operatív hatását. A társjogalkotóktól kapott megbízásnak megfelelően a Bizottság: először is értékelte és felmérte a személyes adatok kezelésére vonatkozó egyes új szabályok **operatív hatását** az Europolnak az Europol-rendelet 3. cikkében meghatározott célkitűzéseivel összefüggésben (nevezetesen: a tagállami illetékes hatóságok tevékenységének, valamint az Europol hatáskörébe tartozó bűncselekmények megelőzése és az ellenük folytatott küzdelem terén megvalósuló kölcsönös együttműködésük támogatása és megerősítése); másodszor értékelte e szabályoknak a Chartában[8] rögzített **alapvető jogokra és szabadságokra** (a továbbiakban: alapvető jogok) gyakorolt hatását, harmadszor pedig elvégezte a kapcsolódó adatkezelési feladatok **költség-haszon elemzését**.

A felülvizsgálat előkészítése érdekében a Bizottság szolgálatai különböző forrásokból gyűjtöttek információkat és visszajelzéseket, valamint eseti konzultációkat folytattak az Europollal és a tagállamokkal. Az e jelentést kísérő **bizottsági szolgálati munkadokumentum** részletesen ismerteti a felülvizsgálat általános kontextusát és módszertanát, valamint átfogóan bemutatja a jelentésben összefoglalt főbb megállapításokat alátámasztó bizonyítékok forrásait és a konzultációkat.

2. Általános kontextus

Az Europol-rendelet 68. cikkének (3) bekezdésével összhangban ez a bizottsági jelentés az (EU) 2022/991 rendelet egyes rendelkezéseire vonatkozik, és az Europol munkájának öt fő aspektusára összpontosít.

1. Külső dimenzió: harmadik országbeli állampolgárokra vonatkozó információs figyelmeztető jelzéseknek a Schengeni Információs Rendszerbe (SIS) való bevitelére vonatkozó, az Europol-rendelet 4. cikke (1) bekezdésének t) pontja alapján az Europol által tett javaslatok

A **súlyos bűncselekmények és a terrorizmus globális jellegére** tekintettel az EU belső biztonsága szempontjából egyre nagyobb jelentőséggel bírnak a harmadik országok és nemzetközi szervezetek birtokában lévő, az elkövetőkre és az ilyen bűncselekményekkel gyanúsított személyekre vonatkozó információk. Az uniós bűnüldözési együttműködés külső dimenziója ezért döntő fontosságúvá vált a tagállamok számára, csakúgy, mint **az Europol szerepe a tagállamok harmadik országokkal** vagy harmadik országokban található szervezetekkel **fenntartott partnerségeinek támogatásában**. **A jövőben** további erőfeszítésekre **lesz szükség** a globális biztonság megerősítése érdekében[9].

Az (EU) 2022/991 rendelet már jelentős módosításokat vezetett be az Europol-rendeletbe **az Europol tevékenységei külső dimenziójának** fokozása érdekében, különös tekintettel a harmadik országokkal folytatott információcsere megkönnyítésére, valamint arra, hogy az Europolnak a többéves programozásába és éves munkaprogramjaiba be kell építenie a

---

7 Ez az Europol-rendelet 68. cikke (3) bekezdésének megfelelően elvégzett értékelés nem azonos a minőségi jogalkotásra vonatkozó iránymutatások szerint elvégzendő, az Europol-rendelet esetleges felülvizsgálatára irányuló javaslatra tekintettel elvégzendő értékeléssel. Lásd az alábbi 4. szakaszt.

8 Az Európai Unió Alapjogi Chartája (HL C 326., 2012.10.26., 391. o., ELI: http://data.europa.eu/eli/treaty/char_2012/oj).

9 Lásd: ProtectEU: Európai belső biztonsági stratégia, COM(2025) 148 final, 2025. április 1., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52025DC0148.

harmadik országokkal[10] és nemzetközi szervezetekkel fenntartott kapcsolatokra vonatkozó stratégiát[11].

Az Europol-rendelet 4. cikke (1) bekezdésének t) pontja új feladattal bízta meg az Europolt: támogatnia kell a tagállamokat a terrorizmusban vagy súlyos bűncselekményekben érintett személyekre vonatkozó, harmadik országok vagy nemzetközi szervezetek által szolgáltatott adatok kezelésében. Ez magában foglalja azt is, hogy **javaslatot tegyen a tagállamoknak arra, hogy harmadik országbeli állampolgárokra vonatkozó, az Unió érdekében álló információs figyelmeztető jelzéseket vigyenek be a Schengeni Információs Rendszerbe (SIS)**. Az információs figyelmeztető jelzések ezen új kategóriáját 2022-ben vezették be[12] a SIS-nek a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén való használatáról szóló (EU) 2018/1862 rendelet[13] módosítását követően.

Bizonyos információkat – különösen akkor, ha az érintett személy nem uniós polgár és nincs kapcsolata valamely nemzeti üggyel – a harmadik ország csak az Europolnak adja át, amely feldolgozza az adatokat és elemzési eredményeit megosztja az összes tagállammal. Az új rendelkezések célja az volt, hogy **maximalizálják** a harmadik országoktól az Europolhoz beérkező **információk kiaknázását** azáltal, hogy azokat könnyebben hozzáférhetővé teszik, mintha csak az Europol saját rendszerén keresztül lennének elérhetők. Ez olyan egyéb intézkedéseket egészített ki, mint az európai keresőportál (ESP) és az EU biztonsági, határigazgatási és migrációkezelési információs rendszerei közötti interoperabilitási keret[14], amelyek a nemzeti hatóságok és különösen a határőrök munkáját akadályozó, ezekkel a rendszerekkel kapcsolatos strukturális hiányosságokat hivatottak orvosolni.

A **SIS kulcsfontosságú kiegészítő terjesztési csatorna**: ez a legszélesebb körben használt figyelőlista Európában a bűnüldözés, a határellenőrzés és a migráció területén. 2024-ben több mint 15 milliárd lekérdezést végeztek a SIS-ben, szemben az illetékes hatóságok számára létrehozott másik két vezető információs rendszerben, az Europol Információs Rendszerben végzett mintegy 14 millió lekérdezéssel és a 19 INTERPOL-adatbázisban (világszerte) végzett kevesebb mint 3 milliárd lekérdezéssel[15].

2. Innováció: Az Europol-rendelet 18. cikke (2) bekezdésének e) pontja és 33a. cikke a személyes adatoknak az Europol által innovációs és kutatási projektek céljából történő kezeléséről

A technológiai fejlemények egyszerre jelentenek hatalmas lehetőségeket és komoly kihívásokat az EU belső biztonsága szempontjából[16], és olyan mélyreható hatást gyakorolnak

---

10 Lásd például az Europol-rendelet 25. cikkének (4a) bekezdését, amely lehetővé teszi az Europol számára, hogy adatokat továbbítson harmadik országoknak, miután az Europol a személyes adatok továbbításának valamennyi körülményét értékelte, és megállapította, hogy a személyes adatok védelme tekintetében megfelelő biztosítékok állnak fenn, valamint a rendelet 25. cikkének (5) bekezdését, amely kiterjeszti azon kivételes esetek hatályát, amikor az Europol kellően indokolt esetekben eseti alapon továbbíthat adatokat harmadik országoknak és nemzetközi szervezeteknek.

11 Az Europol-rendelet 12. cikkének (2) bekezdése.

12 (EU) 2022/1190 rendelet (HL L 185., 2022.7.12., 1. o., ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 (EU) 2018/1862 rendelet (HL L 312., 2018.12.7., 56. o., ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 (EU) 2019/818 rendelet (HL L 135., 2019.5.22., 85. o., ELI: http://data.europa.eu/eli/C/2019/818/oj.

15 Az eu-LISA 2024. évi éves SIS-jelentése online elérhető a következő címen: https://www.eulisa.europa.eu/sites/default/_files/documents/sis-annual-report-2024.pdf, az Europol 2024. évi konszolidált éves tevékenységi jelentése (CAAR) online elérhető a következő címeken: https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF és https://www.interpol.int/How-we-work/Databases.

16 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (Az internetes szervezett bűnözés általi fenyegetettség értékelése [IOCTA] 2024), online elérhető a következő címen: Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

a bűnözésre, amely megváltoztatja a súlyos és szervezett bűnözés fenyegetéseinek mélyebb természetét („DNS”-ét)[17]. A bűnözők gyorsan integrálják az új technológiákat tevékenységükbe, új üzleti modelleket hoznak létre és finomítják taktikáikat. Ugyanakkor ezek a fejlemények **soha nem látott lehetőségeket kínálnak a bűnüldöző szerveknek képességeik fejlesztésére**. Ezért a kutatás és az innováció döntő szerepet játszik a belső biztonságban azáltal, hogy megoldásokat dolgoz ki az új fenyegetésekkel szembeni küzdelemre és arra, hogy lépést tartson a bűnözői hálózatok gyorsan változó formáival és működési módjaival, köztük a technológia visszaélésszerű használatából fakadókkal. Az Unió a **ProtectEU**, az európai belső biztonsági stratégia[18] keretében az uniós finanszírozású biztonsági kutatás és innováció révén beruházott és továbbra be fog ruházni az innovatív eszközök fejlesztésébe.

Az uniós tagállamok bel- és igazságügyi minisztereinek megbízásából 2019 végén létrehozott **Europol Innovációs Labor**[19] célja, hogy előmozdítsa az Europol bűnüldözési innováció iránti elkötelezettségét. Az (EU) 2022/991 rendelet jelentős módosításokat vezetett be az Europol-rendeletbe annak érdekében, hogy egyrészt támogassa az Europol Innovációs Labor potenciálját, másrészt elősegítse a szinergiákat az egyéb uniós szintű, többek között a Bizottságban, a belső biztonság **európai uniós innovációs központja** keretében folyó kutatási és innovációs tevékenységekkel[20].

Az Europol-rendeletnek az információfeldolgozási tevékenységek céljáról szóló 18. cikkének (2) bekezdését módosították annak érdekében, hogy az Europol **kutatási és innovációs projektek céljából** is **kezelhesse a műveleti vonatkozású személyes adatokat**. Az új eszközök érvényességének empirikus tesztelését lehetővé tevő, magas színvonalú adatkészletek rendelkezésre állását széles körben a technológiák fejlesztésének egyik alapvető előfeltételének tekintik. Ezzel szemben a teszteléshez használt megbízhatatlan vagy torzult adatkészletek gyenge minőségű technológiákhoz vezethetnek[21].

Az ilyen adatkezelésre vonatkozó egyedi adatvédelmi biztosítékokat az **Europol-rendelet** 18. cikkének (3a) bekezdése, 30. cikkének (2) és (3) bekezdése, valamint **33a. cikke** tartalmazza. Ez utóbbi cikk olyan **tesztkörnyezet** létrehozását írta elő, amelynek értelmében a projekt keretében kezelt személyes adatokat ideiglenesen át kell másolni az Europolon belül egy különálló, elszigetelt és védett adatfeldolgozási környezetbe, amelyet kizárólag az adott projekt céljára lehet felhasználni.

3. <u>Nyomozások</u>: Az Europol-rendelet 18. cikkének (6a) bekezdése és 18a. cikke az érintettek kategorizálása nélkül kapott személyes adatok kezelésének feltételeiről

Uniós bűnügyi információs központként az Europol nemcsak az információgyűjtést és -cserét könnyíti meg, hanem **fejlett adatelemzéssel**, valamint a bűncselekmények és a nemzeti szinten nem látható, határokon átnyúló bűnözői hálózatok közötti kapcsolatok felderítésével is hozzájárul **a nyomozások hatékonyságának növeléséhez**. Ezek a képességek azáltal támogatják a tagállamokat, hogy gazdagítják a nyomozásokhoz rendelkezésre álló információkat.

A technológia kiterjedt és intenzív használatával a **nagy és összetett adatkészletek az élet minden területén**, így a bűnözés terén is **új normává váltak**[22]. A szervezett bűnözéssel és a terrorizmussal kapcsolatos nyomozások során egyre gyakrabban kell szembenézni azzal a

---

17 Europol, EU SOCTA 2025, 19. o.

18 COM(2025) 148 final, 2025. április 1., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52025DC0148, 9. o.

19 https://www.europol.europa.eu/how-we-work/innovation-lab.

20 Lásd különösen az Europol-rendelet 4. cikke (1) bekezdésének v) és w) pontját.

21 SWD(2020) 543 final, 2020. december 9., 29. o.

22 Europol, EU SOCTA 2025, több helyen.

kihívással, hogy nagy mennyiségű, gyakran több terabájtnyi elektronikusan tárolt adatot – például a nyomozások során lefoglalt hang-, video- és gépi adatokat – kell elemezni. Például az EncroChat hálózat[23] felszámolására irányuló közös nyomozás során a nyomozók több millió olyan üzenetet elemeztek, amelyeket a bűnözők súlyos bűncselekmények tervezése céljából váltottak egymással. Mindezek alapján a bűnüldöző és igazságügyi hatóságok számára kulcsfontosságú a nagy és összetett (a szakzsargonban „big data"[24] néven ismert) adatkészletek elemzéséhez szükséges információs és kommunikációs technológiai (IKT) eszközök, szakértelem és erőforrások rendelkezésre állása.

Bár a 2016-ban elfogadott Europol-rendelet önmagában nem írt elő korlátozásokat a big data elemzésére vonatkozóan, nem tartalmazott strukturált rendelkezéseket, amelyek meghatározták volna az ilyen típusú adatok elemzésének feltételeit. A **legkritikusabb pont az érintettek kategorizálására vonatkozó követelmény** volt. Az érintettek kategorizálása arra utal, hogy az adatok tényleges nyomozási célú feldolgozása – például a kapcsolatok azonosítása céljából végzett keresztellenőrzés, valamint stratégiai vagy tematikus, valamint operatív elemzések elvégzése – előtt az adatkészleteket át kell vizsgálni, hogy a személyes adatokat az Europol-rendelet II.A. és II.B. mellékletében kimerítően felsorolt különböző kategóriák szerint szétválogassák[25]. Az érintett kategóriák a nyomozásokban való érintettség különböző típusaihoz kapcsolódnak, beleértve i. a gyanúsítottakat, a potenciális jövőbeli elkövetőket, valamint ii. a bűncselekményekhez kötődő kapcsolatokat, a bűntársakat, az áldozatokat, a tanúkat és az informátorokat. Az Europol általában nem kezelheti, sőt nem is tárolhatja olyan egyének személyes adatait, akik nem tartoznak e kategóriák egyikébe sem.

Az adatszolgáltatók, például **a tagállamok** vagy **az uniós szervek és ügynökségek jellemzően** már a személyes adatok Europolnak történő továbbítása előtt elvégzik az érintettek kategorizálását[26]. Az uniós jog értelmében – függetlenül az Europol részére történő adattovábbítástól – mindannyian kötelesek elvégezni az érintettek kategorizálását saját adatkezelésük és nyomozásaik céljából, az Europol szabályaival egyenértékű, de nem azonos szabályokat alkalmazva[27]. A nagy és összetett adatkészletek esetében azonban a manuális előfeldolgozás erőforrás- és időigényes feladat. Egyetlen mobiltelefon adatainak elemzése félig automatizált módon akár három napig is eltarthat, és egy nyomozás során akár több száz mobiltelefont is lefoglalhatnak. A **big data** esetében az érintettek kategorizálása **nem mindig lehetséges**, tekintettel az adathalmazok hatalmas mennyiségére, az adatok (nem) strukturált jellegére, az erőforrások hiányára vagy a túlzott mértékű **manuális munkaigényre**. A

---

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochatcommunications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 Az európai adatvédelmi biztos 7/2015. sz. véleménye, 7. o., elérhető a https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf címen. „A »**big data**« a rendelkezésre álló különböző fogalommeghatározások közös nevezőjeként általában azt a gyakorlatot jelenti, hogy hatalmas mennyiségű, különböző forrásból származó információt kombinálnak és elemeznek, kifinomultabb algoritmusokat használva a döntések megalapozására. A big data nemcsak arra támaszkodik, hogy a technológia egyre jobban képes nagy mennyiségű adat gyűjtésére és tárolására, hanem arra is, hogy képes az adatok teljes értékét elemezni, megérteni és kihasználni (különösen elemző alkalmazások segítségével)."

25 Lásd az Europol-rendelet 18. cikkének (2) bekezdését.

26 A tagállamok a Biztonságos Információcsere Hálózati Alkalmazáson (SIENA) keresztül továbbítják az adatokat az Europolnak, ahol az érintettek kategorizálását kötelező mezőként alkalmazzák.

27 Lásd például az (EU) 2016/680 irányelv (a közvetetten illetékes hatóságok tekintetében a bűnüldözésben érvényesítendő adatvédelemről szóló irányelv) 6. cikkét (HL L 119., 2016.5.4., 89. o., ELI: http://data.europa.eu/eli/dir/2016/680/oj); az (EU) 2017/1939 tanácsi rendelet (a továbbiakban: az EPPO-rendelet) 51. cikkét (HL L 283., 2017.10.31., 1. o., ELI: http://data.europa.eu/eli/reg/2017/1939/oj); valamint az (EU) 2018/1727 rendelet (a továbbiakban: az Eurojust-rendelet) 27. cikkének (3) bekezdését (HL L 295., 2018.11.21., 138. o., ELI: http://data.europa.eu/eli/reg/2018/1727/oj).

gyakorlatban az egyetlen lehetőség az, hogy először operatív szempontból mélyebben elemzik az adatokat, vagy – részben automatizált módon – a rendelkezésre álló adatok keresztellenőrzésével keresik meg a kapcsolatokat.

Az (EU) 2022/991 rendelet pontosította azokat a feltételeket, amelyek mellett az érintettek kategorizálása **jogbiztonságot** nyújt a nagy és összetett adatkészletek kezelése tekintetében. Az Europol és az európai adatvédelmi biztos eltérően értelmezte az Europol-rendelet betűjét és szellemét az alkalmazandó adatmegőrzési időszak tekintetében. Az Europol szerint ennek ez az időszak három év; az európai adatvédelmi biztos szerint pedig hat hónap[28]. Új rendelkezésekre volt szükség **a rugalmasság növelése** érdekében is, hogy megfelelő egyensúlyt lehessen teremteni az adatvédelem és a biztonsági szempontok között.

Az Europol-rendelet 18. cikkének (5a) bekezdése az európai uniós adatvédelmi rendelet 73. cikkével összefüggésben először tovább pontosította az érintettek kategorizálásának a 18. cikk (2) bekezdése és a II. melléklet szerinti általános elvét. Az Europol feladata, hogy adott esetben és amennyire lehetséges, **a személyes adatokat egyértelműen hozzárendelje az érintettek egy meghatározott kategóriájához**. A gyakorlatban az Europolnak főszabályként meg kell határoznia a büntetendő cselekményben betöltött pontos szerepet (például azt, hogy egy személy gyanúsított, áldozat vagy csak tanú) minden olyan személy esetében, akinek a személyes adatait kezelik, nem pedig összesített szinten a kezelendő adatfájlban vagy annak egy részében szereplő valamennyi személyre vonatkozóan (például egyszerűen megállapítva, hogy az adatfájl létrehozását eredményező általános körülmények vizsgálata alapján az összes említett személy az Europol hatáskörébe tartozó bűncselekményben vett részt), mielőtt a személyes adatok kezelése megkezdődhet.

Az Europol-rendelet 18. cikkének (6a) bekezdése kifejezetten lehetővé teszi a kapott személyes adatoknak az érintettek kategorizálása nélküli kezelését **legfeljebb 18 hónapig**, amely indokolt esetben, kizárólag **az érintettek kategorizálásának elvégzése céljából** legfeljebb 36 hónappal meghosszabbítható. Az Europol-rendelet 18. cikkének (6a) bekezdése nem utal kifejezetten a nagy és összetett adatkészletekre, hanem általánosabban a „**feltétlen szükségesség**” vizsgálatát írja elő.

Az Europol-rendelet 18a. cikke eltérést biztosít azáltal, hogy lehetővé teszi az Europol számára, hogy **az illetékes hatóságoktól**, az Európai Ügyészségtől (**EPPO**) vagy az **Eurojusttól** kapott személyes adatokat – amennyiben az egy **folyamatban lévő bűnügyi nyomozás** támogatásához szükséges – anélkül kezelje, hogy – amennyiben erre még nem került sor – elvégezné az érintettek kategorizálását, valamint, hogy az érintetteknek az Europol-rendeletben nem felsorolt kategóriáira vonatkozó adatokat is kezeljen. Az Europol **operatív elemzéssel**, illetve kivételes és kellően indokolt esetekben **keresztellenőrzéssel** is feldolgozhatja az adatokat a kapcsolatok vagy más releváns kapcsolatok azonosítása érdekében. Ennek az eltérésnek az volt a célja, hogy kezelje az érintettek kategorizálására vonatkozóan az Europolra, valamint az illetékes hatóságokra, az Európai Ügyészségre és az Eurojustra alkalmazandó szabályok közötti különbségeket.

4. Együttműködés harmadik felekkel: Az Europol-rendeletnek a személyes adatoknak az Europol és magánfelek közötti cseréjéről szóló 26., 26a. és 26b. cikke

A bűnözők egyre gyakrabban élnek vissza magánfelek (határokon átnyúló) – internetalapú, pénzügyi és klasszikus távközlési – szolgáltatásaival. Következésképpen **a magánfelek nagy mennyiségű, a bűnügyi nyomozások szempontjából releváns személyes adattal rendelkeznek**. Különösen az internet hozott létre egy olyan nyilvános teret, amely

[28] https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

gyakorlatilag magánkézben van, ami megnehezíti, hogy a bűnüldözési célú szabályokat online ugyanolyan hatékonyan érvényesítsék, mint offline[29].

Ennek fényében **elengedhetetlenné** vált **a bűnüldöző hatóságok és a magánfelek közötti együttműködés**. A **ProtectEU**-ban, az európai belső biztonsági stratégiában meghatározottak szerint alapvető fontosságú a magánszektorral való partnerségek megerősítése az információcsere megkönnyítése érdekében[30]. A rendőrségi vezetők az Europol jövőjéről szóló közös nyilatkozatukban[31] azt is szorgalmazták, hogy az Europol „**fontos kapuként szolgáljon a magánszervezetektől származó információk megszerzéséhez**". Ezen együttműködés jellege az információmegosztástól és a nyílt forráskódú kereskedelmi adatok biztosításától a kutatási és innovációs projektekben való részvételig, valamint a vállalati működést támogató szolgáltatások nyújtásági terjed[32]. 2025-ben például az Europol a Microsofttal való együttműködés révén sikeresen felszámolta a Lumma Stealer nevű, világszerte a legnagyobb veszélyt jelentő információlopó programot, amely globálisan több mint 394 000 Windows-számítógépet fertőzött meg[33].

Az (EU) 2022/991 rendelet **további lehetőségeket** vezetett be az Europol számára a személyes adatok magánfelekkel való cseréjére. Korábban az Europol csak az Europol nemzeti egységén keresztül vagy harmadik országok vagy nemzetközi szervezetek előre meghatározott kapcsolattartó pontjain vagy hatóságain keresztül kaphatott személyes adatokat magánfelektől. Az Europol adatkezelésének célja az Europol érintett nemzeti egységének, illetve az ügyért felelősséget vállaló harmadik ország vagy nemzetközi szervezet kapcsolattartó pontjának vagy hatóságának azonosítására korlátozódott.

A **módosított Europol-rendelet 26. cikke kibővítette az Europol feladatát**, lehetővé téve számára a magánfelektől származó információk (köztük a személyes adatok) átfogó kezelését. Az adatkezelés elsődleges célja továbbra is az Europol érintett nemzeti egységének azonosítása. Az Europol azonban most már kiegészítheti az információkat saját elemzésével, hogy megkönnyítse az ügy további feldolgozását nemzeti szinten.

Az Europol-rendelet 26. cikkének horizontális rendelkezései mellett az Europol-rendelet 26a. cikke szabályokat vezetett be az **online válsághelyzetekre** vonatkozóan, a 26b. cikk pedig **a gyermekek szexuális bántalmazását ábrázoló anyagok online terjesztésével** foglalkozik. Ezekben az esetekben az Europol segítheti a tagállamokat a magánfelektől közvetlenül kapott személyes adatok feldolgozásával. Eseti alapon az Europol is továbbíthat személyes adatokat magánfeleknek.

Az (EU) 2022/991 rendelet bevezette annak lehetőségét, hogy az Europol infrastruktúráját az illetékes hatóságok és a magánfelek közötti információcserére használják, valamint azt a lehetőséget, hogy az Europol a tagállamoktól kérje, hogy nemzeti jogszabályaiknak megfelelően szerezzenek be személyes adatokat magánszemélyektől.

---

29 SWD(2020) 543 final, 2020. december 9., 16–17. o.

30 Lásd: ProtectEU: Európai belső biztonsági stratégia, 6. o.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Együttműködés magánfelekkel, 2023. május 31., EDOC #1306090v13. Lásd még: Milieu Consulting, Study on the Practice of direct exchange with personal data between Europol and Private Party (Tanulmány a személyes adatoknak az Europol és magánfelek közötti közvetlen cseréjének gyakorlatáról), zárójelentés, 2020. szeptember.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. További példák az e jelentést kísérő bizottsági szolgálati munkadokumentumban találhatók.

Ezeket a rendelkezéseket más kezdeményezésekkel, például az online terrorista tartalomról szóló rendelettel[34] és a digitális szolgáltatásokról szóló rendelettel[35] összhangban fogadták el. A Bizottság további intézkedéseket irányoz elő a magánfelek bűnözés elleni küzdelemben való részvételének fokozására és az adatokhoz való jogszerű hozzáférés megkönnyítésére annak érdekében, hogy az EU a **ProtectEU**, az európai belső biztonsági stratégia keretében megvalósítsa „ a biztonság kultúrájának megváltoztatását" (**a társadalom egészére kiterjedő megközelítés**)[36].

5. Az alapvető jogok Europol általi tiszteletben tartásának belső és külső felügyelete

Az (EU) 2022/991 rendelet hangsúlyozza, hogy az Europolnak tiszteletben kell tartania az alapvető jogokat az Europol feladatait meghatározó rendelkezések és a kapcsolódó megerősített biztosítékok alapján, különösen **az Ügynökség belső és külső felügyeletének megerősítése** révén.

Az adatvédelem területén az Europol-rendeletnek az európai uniós adatvédelmi rendelet szerinti adatvédelmi biztosítékokkal való összehangolása az **adatvédelmi tisztviselő** és az **európai adatvédelmi biztos** általi felügyeletre vonatkozó új szabályok bevezetését vonta maga után. Például az adatvédelmi hatásvizsgálat elvégzésére vonatkozó kötelezettség és az európai adatvédelmi biztossal való előzetes konzultáció minden új típusú adatkezelés esetében szisztematikussá vált. Az (EU) 2022/991 rendelet új hatáskört is bevezetett az Europol számára a hozzáférési jogok iránti kérelmek tekintetében. Korábban az illetékes nemzeti hatóságok voltak felelősek a hozzáférési jogok iránti kérelmek kezeléséért, amennyiben a tagállamok voltak az adatszolgáltatók.

Az (EU) 2022/991 rendelet **új álláshelyet is létrehozott az alapjogi tisztviselő számára** az Europolnál, akinek feladata többek között az, hogy tájékoztassa az Europol ügyvezető igazgatóját az ügynökség tevékenysége során előforduló esetleges alapjogi jogsértésekről.

Emellett az Európai Unió működéséről szóló szerződés (EUMSZ) 88. cikke (2) bekezdésének második albekezdésében előírtak szerint az Europol tevékenységeinek **az Európai Parlament és a nemzeti parlamentek** általi politikai nyomon követése **megerősítette a demokratikus felügyeletet és az elszámoltathatóságot**. Az (EU) 2022/991 rendelet megerősítette a **közös parlamenti ellenőrző csoport** által végzett ellenőrzést[37]. Előírta például, hogy a közös parlamenti ellenőrző csoportnak kötelező konzultációt kell folytatnia az Europol többéves programozásának és éves munkaprogramjának tervezetéről, lehetővé tette számára, hogy nem kötelező erejű konkrét ajánlásokat fogalmazzon meg az Europol számára, és azokat benyújtsa az Európai Parlamentnek és a nemzeti parlamenteknek, valamint előírta egy konzultációs fórum létrehozását, amely kérésre alapjogi kérdésekben független tanácsadást biztosít.

3. Az értékelés főbb megállapításai

3.1. Az Europol új személyesadat-kezelési hatáskörei és feladatai operatív végrehajtásának jelenlegi állása

Az (EU) 2022/991 rendelet **2022. június 28-án lépett hatályba**. Operatív végrehajtása azonban különböző irányítási, technikai és adminisztratív intézkedésektől, valamint operatív követelményektől, például egyes esetekben új IKT-struktúrák létrehozásától függött.

Három évvel később az (EU) 2022/991 rendelet 68. cikkének (3) bekezdésében felsorolt **szinte valamennyi rendelkezés hatályba lépett**. A nagy és összetett adatkészletek elemzésével (az

---

34 (EU) 2021/784 rendelet (HL L 172., 2021.5.17., 79. o., ELI: http://data.europa.eu/eli/reg/2021/784/oj).
35 (EU) 2022/2065 rendelet (HL L 277., 2022.10.27., 1. o., ELI: http://data.europa.eu/eli/reg/2022/2065/oj).
36 Lásd: ProtectEU: Európai belső biztonsági stratégia, 2. o.
37 Lásd: https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

Europol-rendelet 18. cikkének (6a) bekezdése és 18a. cikke) és a magánfelekkel való együttműködéssel (az Europol-rendelet 26., 26a. és 26b. cikke) kapcsolatos rendelkezések 2022. június 28-tól, illetve röviddel azután léptek hatályba. A kutatási és innovációs projektek esetében a személyes adatok kezelése (az Europol-rendelet 18. cikke (2) bekezdésének e) pontja) 2023-ban kezdődött, miután létrehozták az ODIN nevű tesztkörnyezetet az Europol-rendelet 33a. cikke szerinti egyedi adatvédelmi követelményeknek való megfelelés érdekében. 2025. június 29-ig még nem vált működőképessé az Europol azon lehetősége, hogy az Europol-rendelet 4. cikke (1) bekezdésének t) pontjával összhangban **a SIS-ben rögzítendő információs figyelmeztető jelzéseket** javasoljon a tagállamoknak, mivel az új típusú figyelmeztető jelzések technikai megvalósítása még folyamatban van. A működésbe lépés **2026-ban várható**.

3.2. Az Europol új személyesadat-kezelési hatáskörei és feladatai által az Ügynökségnek az Europol-rendelet 3. cikke szerinti célkitűzéseire gyakorolt operatív hatás értékelése

Ami az Europol új személyesadat-kezelési hatásköreinek és feladatainak operatív hatását illeti, a konzultáció azt mutatta, hogy **a tagállamok összességében kedvezően vélekednek** azok relevanciájáról, hatékonyságáról és hozzáadott értékéről, valamint az Europol által az illetékes hatóságaiknak a kapcsolódó területeken nyújtott támogatásról[38].

Az ezen értékelés tárgyát képező nyomozati hatásköröket nem használják fel folyamatosan vagy módszeresen az adatok monitoring céljából történő kezelésére; ezek közül egyesek még kivételes jellegűek is, míg másokat a nyomozások során szükség szerint, rendszeresebben alkalmaznak. A referencia-időszakban **az új rendelkezések operatív alkalmazása mennyiségi szempontból jelentősen eltért**, az új rendelkezésekhez kapcsolódó eltérő technikai jellemzőktől és jogi feltételektől függően.

Az Europol a végrehajtási rendelet 18. cikkének (6a) bekezdése alapján **nem elhanyagolható** számú, **az érintettek kategorizálása nélküli új hozzájárulást** kapott a tagállamoktól, ami 2023-ban 653, 2024-ben pedig 597 hozzájárulást jelentett. Az érintettek kategorizálása nélküli hozzájárulások rövid távon nem növekedtek, és azoknak az eseteknek a száma, ahol a 18. cikk (6a) bekezdését alkalmazták, **állandó** maradt a 2022. június 28. előtti időszak hasonló eseteihez képest. Az új rendelkezések nem gyakoroltak negatív hatást a tagállamoknak az érintettek kategorizálásában[39] való részvételére sem. 2023 és 2024 között az érintettek kategorizálása nélküli hozzájárulások aránya az Europol által a tagállamoktól elfogadott **összes hozzájárulás kevesebb mint 1 %-át** tette ki (0,85 % 2023-ban és 0,71 % 2024-ben). 2022 júniusa óta az Europol következetesen 18 hónapon belül elvégezte az érintettek kategorizálását, a meghosszabbított 36 hónapos időszak kihasználása nélkül. Az Europol és hat tagállam hangsúlyozta, hogy a jogbiztonság javulása ellenére **az adminisztratív terhek továbbra is jelentősek** mind az Europol, mind az illetékes hatóságok számára a személyes adatoknak a bűncselekményben való egyéni részvétel szerinti kategorizálásához szükséges erőfeszítések miatt. Ezt a követelményt az Europol nagyon szigorúan hajtja végre[40].

Az Europol arról számolt be, hogy a **magánfelekkel** folytatott információcsere 2023-ban még mindig elhanyagolható volt, mivel (a digitális szolgáltatásokról szóló rendelet hatálya alá

---

[38] Lásd az e jelentést kísérő bizottsági szolgálati munkadokumentum 5. szakaszában bemutatott bizonyítékokat, különösen az Europol beadványait és a 2025. június 2-i rövid kérdőív 2., 4. és 5. kérdésére adott tagállami válaszokat a bizottsági szolgálati munkadokumentum III. mellékletében.

[39] Amint azt egy tagállam a konzultáció során hangsúlyozta, „[a tagállamok] egyértelműen meg tudják különböztetni, hogy milyen típusú adatokat kezelnek, ami nagyon fontos lehet a nyomozás során”.

[40] Lásd az e jelentést kísérő bizottsági szolgálati munkadokumentum 7.1.3. alszakaszát és a tagállamoknak a 2025. június 2-i rövid kérdőív 9. kérdésére adott válaszait a bizottsági szolgálati munkadokumentum III. mellékletében.

tartozó eseteken kívül) csak 26 esetben került sor az Europol-rendelet 26. cikkének végrehajtására[41]. **2024**-ben azonban a statisztikák **meredeken, 284-re** (közel + 1 000 %-kal) **emelkedtek** az Europol-rendelet 26. cikke szerinti, magánfelekkel való együttműködést magában foglaló ügyekben. Ez különösen igaz volt a magánvállalatoktól származó, a **pénzügyi és gazdasági bűncselekmények** kinyomozására szolgáló adatokra. Az Europol az átdolgozott Europol-rendelet 26b. cikkét is jelentős mértékben alkalmazta a gyermekek szexuális kizsákmányolása elleni küzdelemben, ahol a magánfelekkel folytatott együttműködés már korábban is igen jelentős volt. Az adatok mindkét esetben magukban foglalják azt az együttműködést is, amely a korábbi jogi keret alapján lehetséges volt. A rendelkezésre álló adatokból nem derül ki, hogy ezek az új esetek milyen mértékben tartoznak az új rendelkezések hatálya alá, vagy jelentik a meglévő lehetőségek fokozott kihasználását.

2025-ben az Europol **új stratégiát** fogadott el a magánfelekkel való együttműködés további fokozása érdekében. Ezenkívül intézkedéseket hoztak az Europol IKT-infrastruktúrájának korszerűsítésére, amely az illetékes hatóságok rendelkezésére áll a magánfelekkel való információcsere céljából. **2023**-ban az Europol elindította a *Plateforme Européenne de Retraits de Contenus illégaux sur Internet* (**PERCI**) nevű platformot annak érdekében, hogy megkönnyítse az online terrorista tartalom terjesztésével szembeni fellépésről szóló rendelet és – a jövőben – a digitális szolgáltatásokról szóló rendelet 18. cikkének végrehajtását, valamint *a gyermekbántalmazás-bejelentési uniós szolgálat* (**EU CARES**) megvalósítását. A PERCI nem része az Europol Információs Rendszernek[42].

Más rendelkezéseket egyáltalán **nem alkalmaztak** (az Europol-rendelet 26a. cikke), annak ellenére, hogy azok működőképesek voltak, **vagy csak kivételesen** alkalmazták őket (egy esetben alkalmazták az Europol-rendelet 18a. cikkét 2024-ben, és egy projekt valósult meg a személyes adatoknak a 18. cikk (1) bekezdésének t) pontja szerinti kezelésével kapcsolatban 2025-ben, három új projekt pedig már folyamatban van).

Az (EU) 2022/991 rendelet által bevezetett rendelkezések operatív végrehajtásának korlátozott időtartama, valamint a bűnügyi nyomozások és a bírósági eljárások hosszadalmas jellege miatt a tagállamok nem tudtak mennyiségi adatokat szolgáltatni az említett rendelkezések operatív hatásairól. Ehelyett példákat mutattak be olyan sikeres nyomozásokra, amelyek a már használatban lévő rendelkezések esetében bizonyítják **az új nyomozási lehetőségek kézzelfogható előnyeit a valós helyzetekben**, nevezetesen az EncroChat, a Sky ECC, a kokainkereskedelemben részt vevő balkáni bűnözői hálózatok vagy a Lumma Stealer esetében.

Az Europol és nyolc tagállam néhány **fejlesztendő területet** is megjelölt az új jogi keret hatékony és koherens alkalmazásának maximalizálása, valamint az Europol szerepének erősítése érdekében a jövőben. Aggodalmak merültek fel, különösen az Europol részéről, hogy a jogi rendelkezések túlzott összetettsége, széttagoltsága és hossza eltántoríthatja a gyakorló szakembereket vagy a magánszemélyeket a rendelkezésre álló új eszközök használatától. A tagállamok észrevételei inkább arra vonatkoznak, hogy az Europol milyen módon hajtja végre az adatvédelmi biztosítékokat az európai adatvédelmi biztos felügyelete alatt, ami aláásható bizonyos rendelkezések hatékonyságát és hozzáadott értékét.

3.3. Az Europol új személyesadat-kezelési hatáskörei és feladatai által az alapvető jogokra gyakorolt hatás értékelése

[41] Europol, 2023. évi jelentés az Europol-rendelet 16. cikkének (11) bekezdése alapján.

[42] (EU) 2019/818 rendelet (HL L 135., 2019.5.22., 85. o., ELI: http://data.europa.eu/eli/reg/2019/818/oj).

A Bizottság **nem** talált arra utaló bizonyítékot, hogy a személyes adatok kezelésére vonatkozó új hatáskörök operatív alkalmazása az új személyesadat-kezelési hatáskörök eddigi korlátozott alkalmazásából eredően **negatív hatással lenne az alapvető jogokra**.

Az új személyesadat-kezelési hatáskörökhöz kapcsolódó konkrét adatvédelmi követelmények végrehajtása mellett az Europol fokozatosan megtett minden szükséges intézkedést az alapvető jogokkal kapcsolatos új horizontális felügyeleti mechanizmusok végrehajtása érdekében.

2024-ben az Europol igazgatótanácsa – az új adatvédelmi rendszerhez kapcsolódó utolsó szükséges végrehajtási jogi aktusok egyikeként – elfogadta az adatvédelmi tisztviselőre vonatkozó felülvizsgált végrehajtási szabályokat. Az összegyűjtött bizonyítékok is arra utalnak, hogy az Europol és igazgatótanácsa az Europol adatvédelmi tisztviselőjével és az európai adatvédelmi biztossal együttműködve biztosította a 2022-ben bevezetett **új adatvédelmi biztosítékok szigorú végrehajtását**. Ez a megközelítés első ránézésre hatékonyan megakadályozta, hogy az új személyesadat-kezelési hatáskörök kezdeti alkalmazása negatív hatást gyakoroljon az egyének magánélethez és a személyes adatok védelméhez való jogára vagy beavatkozzon abba. A tagállamok szerint az Europol jelenleg **szilárd adatvédelmi kerettel** rendelkezik, amely elegendő biztosítékot nyújt új hatásköreinek esetleges fokozott gyakorlásához. Hét tagállam azt is hangsúlyozta, hogy ez a keretrendszer a bizalom növelésével **elősegíti az információáramlást**, bár még mindig van mit javítani. Csak egy tagállam fejezett ki negatív véleményt[43].

Az érintettek kategorizálásával kapcsolatos konkrét **kihívások** mellett az Europol és négy tagállam fejlesztésre szoruló területként említette az **adatvédelmi hatásvizsgálathoz** és az európai adatvédelmi biztossal folytatott **előzetes konzultációhoz** kapcsolódó költségeket és időt, amelyeket a gyakorlatban alapértelmezés szerint elvégeznek. Hat tagállam szerint további kihívást jelent **az érintettek hozzáférési kérelmeinek** az Europol általi kezelése, amelyek tekintetében jelenleg az Europol illetékes, még akkor is, ha az adatok tulajdonosa valamely tagállam.

Az **első alapjogi tisztviselőt 2022** decemberében nevezték ki. Megbízatásának első két évében **nem** kapott és nem is nyújtott be **panaszt** az ügyvezető igazgatóhoz. A közös parlamenti ellenőrző csoport továbbra is szorosan figyelemmel kísérte az Europol tevékenységeit, és az új rendelkezések hatálybalépése óta nem adott ki ajánlásokat. Az Európai Parlament **2024** februárjában létrehozta **a közös parlamenti ellenőrző csoport alapjogi konzultatív fórumát**.

3.4. Az Europol új személyesadat-kezelési hatásköreinek és feladatainak költség-haszon elemzése

Tekintettel az (EU) 2022/991 rendelet által bevezetett rendelkezések végrehajtásának korai szakaszára és az azokkal kapcsolatos korlátozott tapasztalatokra, a Bizottság számára **korai** lenne érdemi következtetéseket levonni az új rendelkezésekről egy **költség-haszon elemzés** alapján.

A Bizottság szolgálatai információkat gyűjtöttek az Europoltól az (EU) 2022/991 rendelet operatív végrehajtásával kapcsolatban a felülvizsgálat alatt álló rendelkezések tekintetében eddig felmerült költségekről. Ezek a költségek 2022 és 2025 között összesen mintegy **25 millió EUR**-t tettek ki (az Europol számára elkülönített teljes összeg mintegy 5 %-a[44]), és

[43] Lásd a tagállamoknak a 2025. június 2-i rövid kérdőív 9. kérdésére adott válaszait az e jelentést kísérő bizottsági szolgálati munkadokumentum III. mellékletében.

[44] Ugyanebben az időszakban az Europol számára elkülönített költségvetés összesen mintegy **860 millió EUR**-t tett ki (ami a 2022. évi 192 millió EUR-ról 2025-re fokozatosan 241 millió EUR-ra nőtt). További részletekért lásd a jelentést kísérő bizottsági szolgálati munkadokumentumot.

elsősorban egyszeri költségeket tartalmazott. A tagállamoknál eddig nem merültek fel kifejezetten az (EU) 2022/991 rendelethez kapcsolódó releváns új költségek.

A költségek nagy részét (közel 17 millió EUR-t) az **új IKT-struktúrák fejlesztésébe**, a kutatásra és innovációra vonatkozó rendelkezések végrehajtásába (ODIN tesztkörnyezet), valamint a személyes adatok magánfelekkel való cseréjére szolgáló információs rendszerekbe (PERCI és EU CARES) történő jelentős beruházások tették ki. Az IKT-hoz és a műveletekhez kapcsolódó **humánerőforrás**-költségek az összes kiadás mintegy egyharmadát tették ki (körülbelül 8 millió EUR). **Hosszú távon** a humán erőforrások fogják **a fő ismétlődő költségeket** jelenteni.

Érdemes megjegyezni, hogy a fent említett 8 millió EUR nem tartalmazza sem az információkezelési egység (IMU) humánerőforrás-költségeit, sem pedig a horizontális jellegű (korábbi és új) felügyeleti intézkedésekhez kapcsolódó erőforrásokat, amelyek esetében nem lehetséges az egyedi rendelkezések végrehajtásának szintjén történő bontás. Az ilyen erőforrások költségei nem elhanyagolhatók. 2023-ban például becslések szerint **teljes munkaidős egyenértékben (FTE) kifejezve 60 fő** (az Europol személyzetének közel **5 %**-a) vett részt **bizonyosságot nyújtó/felügyeleti szervek és felügyeleti/tanácsadó szervezetek** tevékenységeiben. Az Europol teljes munkaidős egyenértékben kifejezve 25 főt bízott meg az adatvédelmi felügyeletre és a kapcsolódó, bizonyosságot nyújtó intézkedésekre való reagálásra irányuló feladatokkal. Ez magában foglalja az európai adatvédelmi biztos ajánlásainak nyomon követését, valamint az operatív adatkezeléssel kapcsolatos előzetes konzultációk keretében végzett munkát. Ebből a 25 teljes munkaidős egyenértékből 16 kifejezetten az európai adatvédelmi biztos követelményeivel kapcsolatos tevékenységeket végez. 2025 júniusától az Europol nyolc teljes munkaidős alkalmazottból – köztük az adatvédelmi tisztviselőből – álló külön csapattal rendelkezik az adatvédelem területén.

Az Europol és tizenöt tagállam szerint az új személyesadat-kezelési hatáskörökből és feladatokból – különösen a nagy és összetett adatkészletek elemzéséből, valamint a magánfelekkel való együttműködésből – származó **előnyök** várhatóan jelentősek lesznek, és **meghaladják a kapcsolódó költségeket**. Egyik tagállamnak sem vélekedett másként. A méretgazdaságosságnak és a csökkenő határköltségeknek köszönhetően hosszú távon észszerűen várható némi hatékonyságnövekedés. Egy tagállam hangsúlyozta, hogy „fontos, hogy az Europol biztosítsa a szükséges IKT-erőforrásokat az (EU) 2022/991 rendelet új lehetőségeinek végrehajtásához szükséges eszközök biztosításához és továbbfejlesztéséhez”, amit két másik tagállam és más érdekelt felek is támogattak[45].

Az Europol és öt tagállam véleménye szerint a végrehajtás esetleges **hiányosságait a meglévő irányítási, igazgatási és adatvédelmi kereten** belül is kezelni kell annak érdekében, hogy ne ássák alá az új személyesadat-kezelési feladatok operatív hatását azok felhasználásának késleltetésével vagy korlátozásával. Öt tagállam felvetette, hogy az Europol és igazgatótanácsa az európai adatvédelmi biztos iránymutatása alapján túlságosan óvatosan hajtja végre az adatvédelmi szabályokat. Azt javasolják, hogy a társjogalkotók által biztosított rugalmasságot megfelelően használják ki az Europol feladatai eredményességének és hatékonyságának maximalizálása, valamint relevanciájuk és hosszú távú megtérülésük biztosítása érdekében.

[45] Lásd az e jelentést kísérő bizottsági szolgálati munkadokumentum 5. szakaszában bemutatott bizonyítékokat, különösen az Europol beadványait és a 2025. június 2-i rövid kérdőív 2., 4. és 5. kérdésére adott tagállami válaszokat a bizottsági szolgálati munkadokumentum III. mellékletében, valamint az európai rendőrségi vezetőknek az Europol jövőjéről szóló közös nyilatkozatát.

Az Europol munkamódszereinek és a lehetséges egyszerűsítési területeknek az értékelése nem tartozik az Europol-rendelet 68. cikkének (3) bekezdése szerinti jelentés hatálya alá, és arra az Europol-rendelet 68. cikkének (1) bekezdése szerinti értékelés keretében kerül sor.

4. Következtetések és további lépések

Összességében a Bizottság előzetes főbb megállapításai szerint a tagállamok továbbra is **támogatják az Europol szerepét** azokon a kulcsfontosságú területeken, ahol jelenleg segíti a tagállamokat **a személyes adatok kezelésével kapcsolatos új feladatainak** ellátásával. Az új személyesadat-kezelési hatáskörök **előnyeinek maximalizálása** érdekében azonban egyes érdekelt felek véleménye szerint **kezelni kell az esetleges hatékonysági problémákat**, különösen a meglévő irányítási, igazgatási és adatvédelmi kereten belül. Hasznos lenne továbbá enyhíteni a jogi keret **összetettségét és széttöredezettségét**, ami eltántoríthatja a szakembereket attól, hogy kihasználják az új lehetőségeket.

A Bizottság általában véve nem talált bizonyítékot arra vonatkozóan, hogy az új szabályok **negatív hatást gyakoroltak volna az alapvető jogokra**, különösen a szilárd adatvédelmi biztosítékoknak köszönhetően, amelyek a partnerek bizalmának növelésével szintén megkönnyítik az információáramlást. Egyes tagállamok szerint az Ügynökség a konzervatív megközelítést részesítette előnyben, miközben **megfelelően ki kellene használni a társjogalkotók által biztosított rugalmasságot** az érintettek kategorizálása, az adatvédelmi hatásvizsgálat, az Europol adatvédelmi biztosával folytatott előzetes konzultáció és a hozzáférési jogokra vonatkozó kérelmek kezelése tekintetében.

Tekintettel az (EU) 2022/991 rendeletben előírt új személyesadat-védelmi szabályok általánosságban rövid végrehajtási időszakára, a gyűjtött bizonyítékok azonban nem minden kérdésben meggyőzőek.

A **ProtectEU**, az európai belső biztonsági stratégia[46] keretében a Bizottság bejelentette, hogy az Europol megbízatásának ambiciózus átalakítását fogja javasolni az eszkalálódó biztonsági kihívások kezelése érdekében. A minőségi jogalkotásra vonatkozó iránymutatásaival[47] összhangban a Bizottság megkezdte az Europol-rendelet és az Europol munkamódszereinek értékelésére irányuló előkészületeket, előkészítve az utat **egy 2026-os bizottsági javaslathoz, amelynek célja a politikai iránymutatásokban foglaltaknak megfelelően az Ügynökség operatívabbá tétele**[48]. 2025 júliusában a Bizottság közzétette a véleményezési felhívást[49], és megbízást adott egy külső tanulmány elkészítésére az Europol-rendelet értékelésének és az új javaslat hatásvizsgálatának alátámasztására. Az Europol-rendelet e jelentés elkészítése céljából elvégzett értékelésének célja, hogy hozzájáruljon az említett értékeléshez.

---

46 ProtectEU: Európai belső biztonsági stratégia, 10. o.

47 Lásd: https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en.

48 Ursula von der Leyen: Politikai iránymutatás a hivatalba lépő következő Európai Bizottság számára (2024–2029), e6cd4328-673c-4e7a-8683-f63ffb2cf648_hu.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Bunuldozesi-egyuttmukodes-Az-uj-Europol-rendeletre-iranyulo-javaslat_hu.