UNIA EUROPEJSKA

PARLAMENT EUROPEJSKI **RADA**

Bruksela, 31 sierpnia 2023 r.
(OR. en)

2021/0393 (COD) **PE-CONS 74/22**

COPEN 462
EUROJUST 116
CT 234
ENFOPOL 659
COTER 308
JAI 1734
CODEC 2085

AKTY USTAWODAWCZE I INNE INSTRUMENTY

Dotyczy:	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 oraz decyzji Rady 2005/671/WSiSW w odniesieniu do cyfrowej wymiany informacji w sprawach związanych z terroryzmem

ROZPORZĄDZENIE
PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2023/...

z dnia ...

w sprawie zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 oraz decyzji Rady 2005/671/WSiSW w odniesieniu do cyfrowej wymiany informacji w sprawach związanych z terroryzmem

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 85,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[1],

[1] Stanowisko Parlamentu Europejskiego z dnia 12 lipca 2023 r. dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia …

a także mając na uwadze, co następuje:

(1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1727[1] ustanowiono Eurojust, a także określono jego zadania, właściwość i funkcje.

(2) Decyzja Rady 2005/671/WSiSW[2] stanowi, że w walce z terroryzmem kluczowe znaczenie dla odpowiednich służb ma posiadanie jak najbardziej kompletnych i aktualnych informacji. Decyzja ta zobowiązuje właściwe organy państw członkowskich do przekazywania Eurojustowi informacji dotyczących ścigania sądowego i skazań w sprawach dotyczących przestępstw terrorystycznych, które mają lub mogą mieć wpływ na co najmniej dwa państwa członkowskie.

(3) W wyniku niespójności w wykładni decyzji 2005/671/WSiSW, w niektórych przypadkach informacje nie są przekazywane terminowo, nie są wcale przekazywane, lub nie wszystkie istotne informacje są przekazywane. Eurojust powinien otrzymywać wystarczające informacje pozwalające na identyfikację powiązań między transgranicznymi postępowaniami przygotowawczymi.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1727 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW (Dz.U. L 295 z 21.11.2018, s. 138).

[2] Decyzja Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych (Dz.U. L 253 z 29.9.2005, s. 22).

(4) Pomaganie właściwym organom państw członkowskich w zapewnieniu jak najlepszej koordynacji postępowań przygotowawczych oraz wniesionych i popieranych oskarżeń, w tym w identyfikacji powiązań między tymi postępowaniami przygotowawczymi i oskarżeniami, jest ważnym zadaniem Eurojustu przewidzianym w rozporządzeniu (UE) 2018/1727. Rozporządzenie to umożliwia Eurojustowi przyjmowanie bardziej proaktywnego podejścia i świadczenie lepszych usług na rzecz państw członkowskich, na przykład poprzez sugerowanie wszczęcia postępowania przygotowawczego i identyfikowanie potrzeb w zakresie koordynacji, potencjalnych przypadków wymagających zastosowania zasady *ne bis in idem* oraz luk dotyczących ścigania.

(5) We wrześniu 2019 r. Eurojust utworzył europejski sądowy rejestr antyterrorystyczny na podstawie decyzji 2005/671/WSiSW, którego konkretnym celem jest identyfikacja potencjalnych powiązań między postępowaniami sądowymi prowadzonymi przeciwko osobom podejrzanym o popełnienie przestępstw terrorystycznych oraz wynikających z tych powiązań ewentualnych potrzeb w zakresie koordynacji.

(6) Europejski sądowy rejestr antyterrorystyczny utworzono po przyjęciu rozporządzenia (UE) 2018/1727, w związku z czym rejestr ten nie jest dobrze zintegrowany z infrastrukturą techniczną Eurojustu ani nie ma o nim wzmianki w tym rozporządzeniu. Należy zatem naprawić tę sytuację.

(7) W celu efektywnego zwalczania terroryzmu zasadnicze znaczenie ma prowadzenie między właściwymi organami a agencjami Unii efektywnej wymiany informacji na potrzeby prowadzenia postępowań przygotowawczych lub wnoszenia i popierania oskarżeń dotyczących przestępstw terrorystycznych. Posiadanie jak najpełniejszych i aktualnych informacji ma kluczowe znaczenie.

(8) Organizacje terrorystyczne są w coraz większym stopniu zaangażowane w inne formy poważnej przestępczości i często należą do zorganizowanych sieci przestępczych. Organizacje te angażują się w inne poważne przestępstwa, takie jak handel ludźmi, handel narkotykami, przestępstwa finansowe i pranie pieniędzy. Konieczne jest dokonywanie kontroli krzyżowej postępowań sądowych dotyczących takich poważnych przestępstw.

(9) W celu umożliwienia Eurojustowi identyfikowania powiązań między transgranicznymi postępowaniami sądowymi prowadzonymi przeciwko podejrzanym o przestępstwa terrorystyczne, jak również powiązań między postępowaniami sądowymi prowadzonymi przeciwko podejrzanym o przestępstwa terrorystyczne a informacjami przetwarzanymi przez Eurojust w innych sprawach dotyczących poważnych przestępstw, konieczne jest, aby Eurojust otrzymywał jak najszybciej od właściwych organów krajowych, zgodnie z odnośnymi przepisami niniejszego rozporządzenia, niezbędne informacje umożliwiające mu identyfikowanie tych powiązań w drodze kontroli krzyżowych.

(10) W celu zapewnienia takich danych Eurojustowi właściwe organy krajowe muszą wiedzieć dokładnie, jakiego rodzaju informacje powinny przekazywać, na jakim etapie krajowego postępowania karnego i w jakich sprawach. Właściwe organy krajowe powinny przekazywać informacje Eurojustowi w sposób ustrukturyzowany, zorganizowany, systematyczny i półautomatyczny. Sposób półautomatyczny to sposób, w którym tryb stosowany do przekazywania informacji jest częściowo zautomatyzowany, a częściowo kontrolowany przez człowieka. Oczekuje się, że taki sposób przekazywania informacji znacznie zwiększy jakość i znaczenie informacji otrzymywanych przez Eurojust.

(11) W związku z wymianą danych, przechowywaniem ich i prowadzeniem kontroli krzyżowych znacznie zwiększy się ilość danych przetwarzanych przez Eurojust. Elementy te należy uwzględnić przy określaniu, przy zastosowaniu istniejących procedur i ram, zasobów finansowych, ludzkich i technicznych, potrzebnych Eurojustowi.

(12) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541[1], transponowana do prawa krajowego, stanowi punkt odniesienia dla właściwych organów krajowych w zakresie zdefiniowania przestępstw terrorystycznych.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).

(13) Wymiana wiarygodnych danych identyfikacyjnych ma kluczowe znaczenie, aby Eurojust mógł zidentyfikować powiązania między postępowaniami przygotowawczymi dotyczącymi terroryzmu a postępowaniami sądowymi przeciwko podejrzanym o przestępstwa terrorystyczne. Kluczowe jest również, aby Eurojust mógł tworzyć i przechowywać zbiór danych zapewniający wiarygodną identyfikację osób, wobec których toczą się takie postępowania przygotowawcze lub postępowania sądowe dotyczące terroryzmu. Istotne jest zatem wykorzystywanie danych biometrycznych, biorąc pod uwagę niepewność związaną z danymi alfanumerycznymi, w szczególności w przypadku obywateli państw trzecich, fakt, że podejrzani posługują się niekiedy fałszywymi lub podwójnymi tożsamościami, oraz to, że na etapie postępowania przygotowawczego dane biometryczne często stanowią jedyne powiązanie z podejrzanymi. W związku z tym, w przypadku gdy na mocy prawa krajowego dotyczącego postępowania karnego lub praw procesowych w postępowaniu karnym właściwe organy krajowe przechowują i gromadzą dane biometryczne i są uprawnione do ich przekazywania, organy te powinny mieć możliwość przekazywania takich danych, gdy są one dostępne, Eurojustowi. Ze względu na wrażliwy charakter danych biometrycznych oraz wpływ ich przetwarzania na poszanowanie życia prywatnego i rodzinnego oraz ochronę danych osobowych zapisane w art. 7 i 8 Karty praw podstawowych Unii Europejskiej, dane takie powinny być przekazywane w sposób ściśle zgodny z zasadami konieczności, proporcjonalności i celowości oraz wyłącznie w celu identyfikacji osób, wobec których toczy się postępowanie karne związane z przestępstwami terrorystycznymi.

(14) Ponieważ informacje o istniejących powiązaniach z innymi postępowaniami sądowymi są najbardziej przydatne na wczesnym etapie postępowania przygotowawczego, konieczne jest, aby właściwe organy krajowe przekazywały informacje Eurojustowi, gdy tylko sprawa zostaje przekazana organowi sądowemu zgodnie z prawem krajowym. Sprawę należy uznać za przekazaną organowi sądowemu, jeżeli na przykład organ sądowy jest informowany o toczącym się postępowaniu przygotowawczym, zatwierdza lub nakazuje przeprowadzenie czynności dochodzeniowej lub postanawia wszcząć postępowanie, w zależności od mającego zastosowanie prawa krajowego. Jeśli właściwy organ krajowy jest już świadomy powiązań między postępowaniem karnym w jego państwie członkowskim a postępowaniem karnym w innym państwie członkowskim, powinien poinformować o tym Eurojust.

(15) Biorąc pod uwagę fakt, że w systemach i tradycjach prawnych niektórych państw członkowskich organ sądowy nie nadzoruje postępowań przygotowawczych i jest angażowany dopiero na późniejszych etapach postępowania, niniejsze rozporządzenie nie powinno uniemożliwiać właściwym organom krajowym przekazywania swoim przedstawicielom krajowym informacji na temat postępowań przygotowawczych dotyczących terroryzmu na wcześniejszym etapie, zgodnie z ich prawem krajowym.

(16) Aby zapewnić prawidłowość danych w europejskim sądowym rejestrze antyterrorystycznym, zidentyfikowanie powiązań lub ustalenie tożsamości osób podejrzanych na jak najwcześniejszym etapie postępowania przygotowawczego**,** oraz aby zapewnić dotrzymywanie terminów, właściwe organy krajowe powinny aktualizować przekazane przez siebie informacje. Takie aktualizacje powinny obejmować nowe informacje dotyczące osoby, wobec której prowadzone jest postępowanie przygotowawcze, orzeczenia sądowe, takie jak tymczasowe aresztowanie, wszczęcie postępowania sądowego, uniewinnienia oraz ostateczne decyzje o odmowie ścigania, a także wnioski o współpracę sądową lub zidentyfikowane powiązania z innymi jurysdykcjami.

(17) Właściwe organy krajowe nie powinny być zobowiązane do przekazywania informacji na temat przestępstw terrorystycznych Eurojustowi na jak najwcześniejszym etapie, jeżeli zagrażałoby to toczącym się postępowaniom przygotowawczym lub bezpieczeństwu danej osoby lub gdy byłoby to sprzeczne z podstawowymi interesami bezpieczeństwa danego państwa członkowskiego. Takie odstępstwa od obowiązku przekazywania informacji powinny być stosowane wyłącznie w wyjątkowych okolicznościach i w drodze analizy każdego indywidualnego przypadku. Rozważając zastosowanie takiego odstępstwa, właściwe organy krajowe powinny odpowiednio uwzględnić fakt, że Eurojust przetwarza otrzymane od nich informacje zgodnie z prawem Unii dotyczącym ochrony danych, oraz uwzględnić tajemnicę postępowania sądowego.

(18) Do celów wymiany wrażliwych danych między właściwymi organami krajowymi a Eurojustem i przetwarzania takich danych, aby chronić takie dane przez nieuprawnionym ujawnieniem i cyberatakami, należy korzystać z bezpiecznych połączeń telekomunikacyjnych, takich jak zdecentralizowany system informatyczny lub bezpieczne połączenie telekomunikacyjne, o którym mowa w decyzji Rady 2008/976/WSiSW[1]. Korzystanie z takich kanałów powinno pozostawać bez uszczerbku dla przyszłego postępu technologicznego.

(19) W celu bezpiecznej wymiany danych oraz ochrony integralności komunikacji i wymiany danych, zautomatyzowany system zarządzania sprawami powinien być podłączony do bezpiecznych kanałów komunikacji i spełniać wysokie normy cyberbezpieczeństwa. Takie bezpieczne kanały komunikacji mogą być również wykorzystywane do łączenia zautomatyzowanego systemu zarządzania sprawami z innymi unijnymi systemami informacyjnymi w zakresie, w jakim akty prawne ustanawiające te systemy przewidują dostęp Eurojustu.

[1] Decyzja Rady 2008/976/WSiSW z dnia 16 grudnia 2008 r. w sprawie Europejskiej Sieci Sądowej (Dz.U. L 348 z 24.12.2008, s. 130).

(20) Zdecentralizowany system informatyczny powinien umożliwiać bezpieczną wymianę danych między właściwymi organami krajowymi a Eurojustem, bez angażowania jakiejkolwiek instytucji, organu lub jednostki organizacyjnej Unii w merytoryczną część takiej wymiany. Zdecentralizowany system informatyczny powinien składać się z systemów back-end państw członkowskich i Eurojustu połączonych wzajemnie przez interoperacyjne punkty dostępu. Punkty dostępu zdecentralizowanego systemu informatycznego powinny być oparte na systemie e-CODEX.

(21) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do utworzenia i wykorzystania zdecentralizowanego systemu informatycznego dla spraw objętych zakresem niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[1].

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

(22) Przekazywanie danych nieustrukturyzowanych powoduje konieczność ręcznej interwencji, stwarza dodatkowe obciążenie administracyjne i obniża jakość wyników kontroli krzyżowych. Dlatego też właściwe organy krajowe powinny przekazywać dane w sposób ustrukturyzowany przy zachowaniu minimalnych wymogów dotyczących interoperacyjności określonych w europejskich ramach interoperacyjności, o których mowa w komunikacie Komisji z dnia 23 marca 2017 r. zatytułowanym „Europejskie Ramy Interoperacyjności – strategia wdrażania". Ponadto przekazywanie danych powinno być jak najbardziej zautomatyzowane, aby zmniejszyć obciążenie administracyjne właściwych organów krajowych oraz zapewnić regularne i szybkie przekazywanie niezbędnych danych.

(23) Zmodernizowany zautomatyzowany system zarządzania sprawami jest niezbędny do tego, aby Eurojust mógł bezpiecznie przetwarzać wrażliwe dane osobowe. Nowy system powinien uwzględniać funkcje europejskiego sądowego rejestru antyterrorystycznego i umożliwiać korzystanie z nich oraz poprawić możliwości Eurojustu w zakresie wykrywania powiązań, korzystając przy tym w pełni z istniejących krajowych i unijnych mechanizmów porównywania danych biometrycznych.

(24) Ważne jest utrzymanie kontroli przedstawicieli krajowych nad danymi, które otrzymują od właściwych organów krajowych oraz ich odpowiedzialności za te dane. Operacyjne dane osobowe nie powinny być przekazywane innemu państwu członkowskiemu domyślnie. Operacyjne dane osobowe należy przekazywać jedynie w zakresie, w jakim właściwe organy krajowe zezwalają na wymianę danych. W celu cyfryzacji i przyspieszenia działań następczych w związku z potencjalnymi powiązaniami, przy jednoczesnym zapewnieniu pełnej kontroli nad danymi, należy wprowadzić kody postępowania.

(25) Obecnie terroryzm oraz poważna i zorganizowana przestępczość są bardzo dynamicznymi i zglobalizowanymi zjawiskami, które często dotyczą dwóch lub większej liczby państw członkowskich. Choć terroryzm miał już silny wymiar ponadnarodowy, wykorzystywanie i dostępność komunikacji elektronicznej sprawiły, że ponadnarodowa współpraca między przestępcami terrorystycznymi znacznie się zwiększyła. Ponadnarodowy charakter przestępstwa terrorystycznego może nie być znany w momencie przekazania sprawy do organu sądowego, ale może zostać stwierdzony podczas kontroli krzyżowych danych przeprowadzanych przez Eurojust. Prowadzenie postępowań przygotowawczych dotyczących przestępstw terrorystycznych lub ściganie tych przestępstw wymaga w związku z tym koordynacji i współpracy między organami ścigania lub wymaga wspólnego ścigania, jak przewidziano w art. 85 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Informacje na temat spraw związanych z terroryzmem powinny być przekazywane do Eurojustu w sposób terminowy, chyba że szczególne okoliczności sprawy wskazują wyraźnie na ich wyłącznie krajowy charakter.

(26) Brak wymiany informacji między krajowymi organami śledczymi i organami ścigania często utrudnia postępowania przygotowawcze oraz wnoszenie i popieranie oskarżeń w sprawach związanych z terroryzmem. Aby móc przeprowadzać kontrole krzyżowe nowych postępowań przygotowawczych w sprawie terroryzmu z wcześniejszymi postępowaniami przygotowawczymi i ustalać potencjalne powiązania, konieczne jest zapewnienie, by okres zatrzymywania danych dotyczących wszelkich wcześniejszych postępowań przygotowawczych oraz wyroków skazujących był odpowiedni względem działań operacyjnych. Dlatego też konieczne jest przedłużenie terminów przechowywania danych w europejskim sądowym rejestrze antyterrorystycznym.

(27) Możliwość przeprowadzenia kontroli krzyżowej nowych postępowań przygotowawczych w sprawie terroryzmu z wcześniejszymi postępowaniami przygotowawczymi może doprowadzić do ustalenia możliwych powiązań i stwierdzenia potrzeby współpracy. Taka kontrola krzyżowa może ujawnić, że osoba podejrzana lub oskarżona w związku z toczącą się sprawą w jednym państwie członkowskim była podejrzana lub oskarżona w związku z zakończoną już sprawą w innym państwie członkowskim. Może ona również pozwolić na ustalenie powiązań między toczącymi się postępowaniami przygotowawczymi lub wniesionymi i popieranymi oskarżeniami, które to powiązania w przeciwnym razie mogłyby pozostać niewykryte. Ma to zastosowanie nawet wtedy, gdy poprzednie postępowania przygotowawcze zakończyły się uniewinnieniem lub ostateczną decyzją o odmowie ścigania. W związku z tym w stosownych przypadkach konieczne jest przechowywanie danych dotyczących wszelkich wcześniejszych postępowań przygotowawczych, nie tylko wyroków skazujących.

(28) Należy zapewnić, aby dane pochodzące z postępowań przygotowawczych, które zakończyły się uniewinnieniem lub ostateczną decyzją o odmowie ścigania, były przetwarzane jedynie do celów ścigania. Danych tych nie można wykorzystywać do celów innych niż identyfikowanie powiązań z toczącymi się postępowaniami przygotowawczymi oraz wniesionymi i popieranymi oskarżeniami oraz wspieranie tych postępowań i oskarżeń. O ile właściwy organ krajowy nie postanowi inaczej w poszczególnych przypadkach, Eurojust powinien mieć możliwość dalszego przetwarzania takich danych operacyjnych. Jeżeli właściwy organ krajowy zdecyduje, że nie jest konieczne przetwarzanie danych osób uniewinnionych lub osób, wobec których odmówiono ścigania, po tym jak odnośne decyzje stały się ostateczne, w tym ze względu na specyfikę sprawy lub podstawy uniewinnienia lub odmowy ścigania, dane takie należy usunąć.

(29) Eurojust zawarł 12 umów o współpracy z państwami trzecimi, które pozwalają na przekazywanie operacyjnych danych osobowych i oddelegowanie do Eurojustu prokuratorów łącznikowych z państw trzecich. Ponadto umowa o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony[1] pozwala na oddelegowanie prokuratora łącznikowego. W marcu 2021 r. Rada upoważniła Komisję do negocjowania umów o współpracy między Eurojustem a 13 kolejnymi państwami trzecimi, a mianowicie Algierią, Argentyną, Armenią, Bośnią i Hercegowiną, Brazylią, Egiptem, Izraelem, Jordanią, Kolumbią, Libanem, Marokiem, Tunezją i Turcją.

[1] Dz.U. L 149 z 30.4.2021, s. 10.

(30) Mimo iż rozporządzenie (UE) 2018/1727 stanowi podstawę prawną do współpracy i wymiany danych z państwami trzecimi, nie zawiera ono jednak żadnych przepisów dotyczących formalnych i technicznych aspektów współpracy z prokuratorami łącznikowymi z państw trzecich oddelegowanymi do Eurojustu, w szczególności w zakresie ich dostępu do zautomatyzowanego systemu zarządzania sprawami. W interesie pewności prawa w rozporządzeniu (UE) 2018/1727 należy zapewnić wyraźną podstawę prawną współpracy między Eurojustem a prokuratorami łącznikowymi z państw trzecich oraz ich dostępu do zautomatyzowanego systemu zarządzania sprawami. Eurojust powinien wprowadzić odpowiednie zabezpieczenia i środki bezpieczeństwa w celu ochrony danych i praw podstawowych za pomocą zaktualizowanej konfiguracji technicznej i rygorystycznych przepisów wewnętrznych.

(31) Przetwarzając operacyjne dane osobowe zgodnie z niniejszym rozporządzeniem, Eurojust powinien zapewnić wysoki poziom ochrony danych. W odniesieniu do przetwarzania operacyjnych danych osobowych Eurojust podlega przepisom art. 3 i rozdziału IX rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[1], a także przepisom szczegółowym dotyczącym przetwarzania operacyjnych danych osobowych przewidzianym w rozporządzeniu (UE) 2018/1727 zmienionym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/838[2] oraz niniejszym rozporządzeniem. Przepisy te mają zastosowanie do przetwarzania wszystkich operacyjnych danych osobowych przetwarzanych przez Eurojust. W szczególności mają one zastosowanie do wszystkich operacyjnych danych osobowych przetwarzanych w zautomatyzowanym systemie zarządzania sprawami, niezależnie od tego, czy są one przetwarzane przez przedstawicieli krajowych, korespondentów krajowych, prokuratorów łącznikowych czy inne upoważnione osoby zgodnie z rozporządzeniem (UE) 2018/1727.

(32) Decyzje dotyczące tego, czy i w jaki sposób Eurojust powinien wspierać koordynację i współpracę między organami prowadzącymi postępowania przygotowawcze i organami właściwymi w zakresie wnoszenia i popierania oskarżeń, powinny pozostać wyłącznie w gestii właściwych organów zainteresowanych państw członkowskich, z zastrzeżeniem mającego zastosowanie prawa krajowego, prawa unijnego lub prawa międzynarodowego, w tym konwencji lub innych umów międzynarodowych o wzajemnej pomocy w sprawach karnych.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/838 z dnia 30 maja 2022 r. w sprawie zmiany rozporządzenia (UE) 2018/1727 w odniesieniu do zabezpieczania, analizy i przechowywania w Eurojuście dowodów dotyczących ludobójstwa, zbrodni przeciwko ludzkości, zbrodni wojennych oraz powiązanych przestępstw (Dz.U. L 148 z 31.5.2022, s. 1).

(33) W celu zapewnienia pewności prawa należy doprecyzować związek między wymianą informacji dotyczących spraw związanych z terroryzmem między właściwymi organami krajowymi a Eurojustem na podstawie decyzji 2005/671/WSiSW i na podstawie rozporządzenia (UE) 2018/1727. W związku z tym z decyzji 2005/671/WSiSW należy usunąć odpowiednie przepisy i dodać je do rozporządzenia (UE) 2018/1727.

(34) Podczas gdy niektóre właściwe organy krajowe są już podłączone do bezpiecznego połączenia telekomunikacyjnego, o którym mowa w art. 9 decyzji 2008/976/WSiSW, wiele właściwych organów krajowych nie jest jeszcze podłączonych do tego bezpiecznego połączenia telekomunikacyjnego ani do bezpiecznych kanałów komunikacji. Aby zagwarantować państwom członkowskim wystarczająco dużo czasu na zapewnienie właściwym organom krajowym takiego połączenia, należy wprowadzić okres przejściowy na wdrożenie.

(35) Zgodnie z art. 1 i 2 oraz art. 4a ust. 1 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej (TUE) i do TFUE, bez uszczerbku dla art. 4 tego protokołu, Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.

(36) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do TFUE, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje,

(37) Zgodnie z art. 42 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 26 stycznia 2022 r.,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Zmiany w rozporządzeniu (UE) 2018/1727

W rozporządzeniu (UE) 2018/1727 wprowadza się następujące zmiany:

1) art. 3 ust. 5 otrzymuje brzmienie:

„5. Eurojust może także udzielać pomocy w postępowaniach przygotowawczych oraz wnoszeniu i popieraniu oskarżeń w sprawach dotyczących tylko państwa członkowskiego i państwa trzeciego lub państwa członkowskiego i organizacji międzynarodowej, o ile z przedmiotowym państwem trzecim lub przedmiotową organizacją międzynarodową została zawarta umowa o współpracy lub porozumienie ustanawiające współpracę na podstawie art. 52 lub o ile w konkretnym przypadku istnieją szczególne powody do udzielenia takiej pomocy.

Decyzja o tym, czy i w jaki sposób państwa członkowskie udzielają pomocy sądowej państwu trzeciemu lub organizacji międzynarodowej, pozostaje wyłącznie w gestii właściwego organu zainteresowanego państwa członkowskiego, z zastrzeżeniem mającego zastosowanie prawa krajowego, unijnego lub międzynarodowego.”;

2) w art. 20 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„2a. Każde państwo członkowskie wyznacza właściwy organ krajowy jako krajowego korespondenta Eurojustu do spraw terroryzmu. Tym krajowym korespondentem do spraw terroryzmu jest organ sądowy lub inny właściwy organ. Jeżeli wymaga tego krajowy system prawny, państwo członkowskie ma możliwość wyznaczenia więcej niż jednego właściwego organu krajowego jako krajowego korespondenta Eurojustu do spraw terroryzmu. Krajowy korespondent do spraw terroryzmu ma dostęp do wszystkich istotnych informacji zgodnie z art. 21a ust. 1. Jest on uprawniony do gromadzenia takich informacji i przesyłania ich Eurojustowi zgodnie z prawem krajowym i prawem Unii, w szczególności z krajowym prawem karnym procesowym i mającymi zastosowanie przepisami o ochronie danych.”;

b) ust. 8 otrzymuje brzmienie:

„8. Dla osiągnięcia celów, o których mowa w ust. 7 niniejszego artykułu, osoby, o których mowa w ust. 3 lit. a), b) i c) niniejszego artykułu, są podłączone do zautomatyzowanego systemu zarządzania sprawami zgodnie z niniejszym artykułem oraz z art. 23, 24, 25 i 34. Koszt podłączenia do zautomatyzowanego systemu zarządzania zostanie pokryty z budżetu ogólnego Unii.”;

3) w art. 21 wprowadza się następujące zmiany:

a) ust. 9 otrzymuje brzmienie:

„9. Niniejszy artykuł nie ma wpływu na inne obowiązki dotyczące przekazywania informacji Eurojustowi.”;

b) ust. 10 otrzymuje brzmienie:

„10. Właściwe organy krajowe nie mają obowiązku udzielania informacji, o których mowa w niniejszym artykule, jeżeli takie informacje zostały już przekazane Eurojustowi zgodnie z innymi przepisami niniejszego rozporządzenia.”;

4) dodaje się artykuł w brzmieniu:

„*Artykuł 21a*

Wymiana informacji dotyczących spraw związanych z terroryzmem

1. W odniesieniu do przestępstw terrorystycznych właściwe organy krajowe informują swoich przedstawicieli krajowych o wszelkich toczących się lub zakończonych postępowaniach przygotowawczych nadzorowanych przez organy sądowe, niezwłocznie po przekazaniu sprawy organom sądowym zgodnie z prawem krajowym, w szczególności krajowym prawem karnym procesowym, o wszelkich toczących się lub zakończonych oskarżeniach i toczących się lub zakończonych postępowaniach sądowych oraz o wszelkich orzeczeniach sądowych dotyczących przestępstw terrorystycznych. Obowiązek ten ma zastosowanie do wszystkich postępowań przygotowawczych dotyczących przestępstw terrorystycznych, niezależnie od tego, czy wykryto powiązanie z innym państwem członkowskim lub państwem trzecim, chyba że dane postępowanie przygotowawcze, ze względu na swoje szczególne okoliczności, wyraźnie dotyczy tylko jednego państwa członkowskiego.

2. Ust. 1 nie ma zastosowania, jeżeli:

   a) wymiana informacji mogłaby zagrozić toczącemu się postępowaniu przygotowawczym lub bezpieczeństwu poszczególnych osób; lub

   b) wymiana informacji byłaby sprzeczna z żywotnymi interesami bezpieczeństwa danego państwa członkowskiego.

3. Do celów niniejszego artykułu przestępstwa terrorystyczne są przestępstwami, o których mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541[*].

4. Informacje przekazywane zgodnie z ust. 1 obejmują operacyjne dane osobowe i dane nieosobowe wymienione w załączniku III. Informacje takie mogą obejmować dane osobowe zgodnie z załącznikiem III lit. d), ale jedynie wtedy, gdy zgodnie z prawem krajowym takie dane osobowe znajdują się w posiadaniu właściwych organów krajowych lub mogą być im przekazane i jeżeli przekazanie tych danych jest niezbędne do wiarygodnej identyfikacji osoby, której dane dotyczą, na podstawie art. 27 ust. 5.

5. Z zastrzeżeniem ust. 2 właściwe organy krajowe informują swoich przedstawicieli krajowych o wszelkich zmianach w informacjach przekazanych na podstawie ust. 1, bez zbędnej zwłoki i, w miarę możliwości, nie później niż 10 dni roboczych po zaistnieniu tych zmian.

6. Właściwy organ krajowy nie ma obowiązku udzielania takich informacji, jeżeli zostały już one przekazane Eurojustowi.

7. Właściwy organ krajowy może na każdym etapie zwrócić się do Eurojustu o udzielenie wsparcia w przeprowadzeniu działań następczych w związku z powiązaniami zidentyfikowanymi na podstawie informacji przekazanych na mocy niniejszego artykułu.”;

---

* Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.U. L 88 z 31.3.2017, s. 6).”;

5) dodaje się artykuły w brzmieniu:

„*Artykuł 22a*

Bezpieczna komunikacja cyfrowa oraz wymiana danych między właściwymi organami krajowymi a Eurojustem

1. Komunikacja między właściwymi organami krajowymi a Eurojustem na podstawie niniejszego rozporządzenia odbywa się za pośrednictwem zdecentralizowanego systemu informatycznego. Zautomatyzowany system zarządzania sprawami, o którym mowa w art. 23, jest podłączony do sieci systemów informatycznych i interoperacyjnych punktów dostępu e-CODEX, za których działanie i za zarządzanie którymi odpowiadają indywidualnie poszczególne państwa członkowskie i Eurojust, która to sieć umożliwia bezpieczną i niezawodną transgraniczną wymianę informacji. (zwany dalej „zdecentralizowanym systemem informatycznym”).

2. W przypadku gdy wymiana informacji zgodnie z ust. 1 nie jest możliwa ze względu na niedostępność zdecentralizowanego systemu informatycznego lub ze względu na wystąpienie wyjątkowych okoliczności, odbywa się ona z wykorzystaniem najszybszych i najbardziej odpowiednich środków alternatywnych. Państwa członkowskie i Eurojust zapewniają, aby alternatywne środki komunikacji były niezawodne i zapewniały równoważny poziom bezpieczeństwa i ochrony danych.

3. Właściwe organy krajowe przekazują Eurojustowi informacje z rejestrów krajowych, o których to informacjach mowa w art. 21 i 21a niniejszego rozporządzenia, w sposób półautomatyczny i ustrukturyzowany. Warunki takiego przekazywania określa Komisja, w porozumieniu z Eurojustem, w drodze aktu wykonawczego, zgodnie z art. 22b niniejszego rozporządzenia. W szczególności taki akt wykonawczy określi format danych przekazywanych na podstawie załącznika III lit. d) do niniejszego rozporządzenia oraz niezbędne standardy techniczne w odniesieniu do przekazywania takich danych, a także określi cyfrowe standardy proceduralne zdefiniowane w art. 3 pkt 9 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/850[*].

4. Komisja powinna być odpowiedzialna za tworzenie, utrzymanie i rozwój oprogramowania wzorcowego, o korzystaniu którego jako ich system back-end państwa członkowskie i Eurojust mogą zdecydować. To oprogramowanie wzorcowe powinno mieć strukturę modułową, co oznacza, że powinno być oprogramowaniem pakietowym dostarczanym niezależnie od elementów systemu e-CODEX niezbędnych do podłączenia tego oprogramowania do zdecentralizowanego systemu informatycznego. Dzięki tej strukturze państwa członkowskie powinny mieć możliwość wykorzystywania lub usprawnienia swoich istniejących krajowych infrastruktur komunikacji sądowej na potrzeby zastosowań transgranicznych, a Eurojust – podłączenia swojego zautomatyzowanego systemu zarządzania sprawami do zdecentralizowanego systemu informatycznego.

5. Komisja bezpłatnie udostępnia, utrzymuje i wspiera oprogramowanie wzorcowe. Utworzenie, utrzymanie i rozwój oprogramowania wzorcowego finansowane są z budżetu ogólnego Unii.

6. Państwa członkowskie i Eurojust pokrywają przypadające na nie koszty ustanowienia i obsługi wyznaczonego punktu dostępu e-CODEX zdefiniowanego w art. 3 pkt 3 rozporządzenia (UE) 2022/850 oraz koszty ustanowienia i dostosowania swoich systemów informatycznych w celu zapewnienia ich interoperacyjności z punktami dostępu.

Artykuł 22b

Przyjmowanie aktów wykonawczych przez Komisję

1. Komisja przyjmuje akty wykonawcze niezbędne do utworzenia i użytkowania zdecentralizowanego systemu informatycznego na potrzeby komunikacji na podstawie niniejszego rozporządzenia, w których określa:

   a) specyfikacje techniczne określające metody komunikacji elektronicznej na potrzeby zdecentralizowanego systemu informatycznego;

   b) specyfikacje techniczne protokołów komunikacyjnych;

c) cele w zakresie bezpieczeństwa informacji oraz odpowiednie środki techniczne zapewniające minimalne normy bezpieczeństwa informacji i normy dotyczące wysokiego poziomu cyberbezpieczeństwa w zakresie przetwarzania i przesyłania informacji w ramach zdecentralizowanego systemu informatycznego;

d) minimalne cele związane z dostępnością i ewentualne związane z tym wymogi techniczne dotyczące usług zapewnianych przez zdecentralizowany system informatyczny;

e) ustanowienie komitetu sterującego składającego się z przedstawicieli państw członkowskich w celu zapewnienia działania i utrzymania zdecentralizowanego systemu informatycznego z myślą o osiągnięciu celów niniejszego rozporządzenia.

2. Akty wykonawcze, o których mowa w ust. 1 niniejszego artykułu, przyjmuje się do dnia … [2 lata od daty wejścia w życie niniejszego rozporządzenia zmieniającego] zgodnie z procedurą sprawdzającą, o której mowa w art. 22c ust. 2.

Artykuł 22c

Procedura komitetowa

1. Komisję wspiera komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 182/2011[**].

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

   W przypadku gdy komitet nie wyda żadnej opinii, Komisja nie przyjmuje projektu aktu wykonawczego i stosuje się art. 5 ust. 4 akapit trzeci rozporządzenia (UE) nr 182/2011.

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/850 z dnia 30 maja 2022 r. w sprawie informatycznego systemu transgranicznej elektronicznej wymiany danych w obszarze współpracy sądowej w sprawach cywilnych i współpracy wymiarów sprawiedliwości w sprawach karnych (system e-CODEX) oraz w sprawie zmiany rozporządzenia (UE) 2018/1726 (Dz.U. L 150 z 1.6.2022, s. 1).

[**] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).”;

6) art. 23, 24 i 25 otrzymują brzmienie:

„*Artykuł 23*
Zautomatyzowany system zarządzania sprawami

1. Eurojust tworzy zautomatyzowany system zarządzania sprawami do celów przetwarzania operacyjnych danych osobowych wymienionych w załączniku II, danych wymienionych w załączniku III oraz danych nieosobowych.

2. Zautomatyzowany system zarządzania sprawami ma następujące cele:

   a) wspieranie prowadzenia i koordynacji postępowań przygotowawczych oraz wniesionych i popieranych oskarżeń w przypadkach, w których Eurojust udziela pomocy;

   b) zapewnianie bezpiecznego dostępu do informacji oraz bezpiecznej wymiany informacji na temat toczących się postępowań przygotowawczych oraz wniesionych i popieranych oskarżeń;

   c) umożliwianie kontroli krzyżowej informacji i wykrycia powiązań;

   d) umożliwianie pobierania danych do celów operacyjnych i statystycznych;

   e) ułatwianie monitorowania w celu zapewnienia, aby przetwarzanie operacyjnych danych osobowych było zgodne z prawem w tym z niniejszym rozporządzeniem oraz z mającymi zastosowanie przepisami o ochronie danych.

3. Zautomatyzowany system zarządzania sprawami może być podłączony do bezpiecznego połączenia telekomunikacyjnego, o którym mowa w art. 9 decyzji Rady 2008/976/WSiSW[*], oraz do innych bezpiecznych kanałów komunikacji zgodnie z mającym zastosowanie prawem Unii.

4. W przypadku gdy Eurojustowi przyznano dostęp do danych znajdujących się w innych unijnych systemach informacyjnych ustanowionych na mocy innych aktów prawnych Unii lub do danych pochodzących z takich systemów, może on korzystać z zautomatyzowanego systemu zarządzania sprawami, aby uzyskać dostęp do danych w tych systemach informacyjnych lub podłączyć się do tych systemów informacyjnych w celu wyszukiwania i przetwarzania informacji, w tym danych osobowych, pod warunkiem że jest to niezbędne do wykonywania jego zadań i zgodne z aktami prawnymi Unii ustanawiającymi takie systemy informacyjne.

5. Ust. 3 i 4 nie rozszerzają uprawnień dostępu do innych unijnych systemów informacyjnych przyznanych Eurojustowi na podstawie aktów prawnych Unii ustanawiających te systemy.

6. Wykonując swoje obowiązki, przedstawiciele krajowi mogą przetwarzać dane osobowe dotyczące indywidualnych spraw, nad którymi pracują, zgodnie z niniejszym rozporządzeniem lub innymi mającymi zastosowanie instrumentami. Udzielają oni inspektorowi ochrony danych dostępu do danych osobowych przetwarzanych w zautomatyzowanym systemie zarządzania sprawami.

7. Do celów przetwarzania operacyjnych danych osobowych Eurojust nie może tworzyć żadnych innych zautomatyzowanych plików danych niż zautomatyzowany system zarządzania sprawami.

Przedstawiciele krajowi mogą tymczasowo przechowywać i analizować dane osobowe do celów ustalenia, czy takie dane są istotne dla zadań Eurojustu i czy mogą zostać włączone do zautomatyzowanego systemu zarządzania sprawami. Dane te można zatrzymać przez okres nie dłuższy niż trzy miesiące.

Artykuł 24

Zarządzanie informacjami w zautomatyzowanym systemie zarządzania sprawami

1. Przedstawiciel krajowy przechowuje w zautomatyzowanym systemie zarządzania sprawami informacje przekazane temu przedstawicielowi krajowemu zgodnie z niniejszym rozporządzeniem lub innymi mającymi zastosowanie instrumentami.

Przedstawiciel krajowy ponosi odpowiedzialność za zarządzanie danymi, które przetwarza.

2. Przedstawiciel krajowy decyduje w poszczególnych przypadkach, czy dostęp do tych informacji powinien pozostać ograniczony, czy też należy udostępnić je w całości lub części innym przedstawicielom krajowym, prokuratorom łącznikowym oddelegowanym do Eurojustu, upoważnionym pracownikom Eurojustu lub innej osobie pracującej w imieniu Eurojustu, która otrzymała niezbędne do tego upoważnienie dyrektora administracyjnego.

3. Przedstawiciel krajowy określa, w porozumieniu z właściwymi organami krajowymi, w sposób ogólny lub szczegółowy wszelkie ograniczenia dotyczące dalszego postępowania z informacjami, dostępu do nich i ich przekazywania, jeżeli stwierdzono istnienie powiązania, o którym mowa w art. 23 ust. 2 lit. c).

Artykuł 25

Dostęp do zautomatyzowanego systemu zarządzania sprawami na szczeblu krajowym

1. Osoby, o których mowa w art. 20 ust. 3 lit. a), b) i c), mają jedynie dostęp do następujących danych:

   a) dane kontrolowane przez przedstawiciela krajowego państwa członkowskiego, z którego osoby te pochodzą;

   b) dane kontrolowane przez przedstawicieli krajowych innych państw członkowskich, do których to danych udzielono dostępu przedstawicielowi krajowemu państwa członkowskiego, z którego osoby te pochodzą, chyba że przedstawiciel krajowy, który kontroluje te dane, odmówił dostępu.

2. W ramach ograniczeń określonych w ust. 1 niniejszego artykułu przedstawiciel krajowy decyduje o tym, w jakim zakresie w jego państwie członkowskim zezwala się na dostęp osobom, o których mowa w art. 20 ust. 3 lit. a), b) i c).

3. Na szczeblu krajowym dostęp do danych przekazywanych zgodnie z art. 21a mogą mieć wyłącznie krajowi korespondenci Eurojustu do spraw terroryzmu, o których mowa w art. 20 ust. 3 lit. c).

4. Każde państwo członkowskie może zdecydować, po konsultacji ze swoim przedstawicielem krajowym, że osoby, o których mowa w art. 20 ust. 3 lit. a), b) i c), mogą – w granicach określonych w ust. 1, 2 i 3 niniejszego artykułu – wprowadzać do zautomatyzowanego systemu zarządzania sprawami informacje dotyczące ich państwa członkowskiego. Taki wkład podlega zatwierdzeniu przez odpowiedniego przedstawiciela krajowego. Kolegium określa szczegóły praktycznego wdrażania niniejszego ustępu. Państwa członkowskie powiadamiają Eurojust i Komisję o decyzjach, jakie podjęły w odniesieniu do wdrożenia niniejszego ustępu. Komisja informuje o tych decyzjach pozostałe państwa członkowskie.

---

* Decyzja Rady 2008/976/WSiSW z dnia 16 grudnia 2008 r. w sprawie Europejskiej Sieci Sądowej (Dz.U. L 348 z 24.12.2008, s. 130).”;

7) w art. 27 wprowadza się następujące zmiany:

a) ust. 4 otrzymuje brzmienie:

„4. Eurojust może przetwarzać szczególne kategorie operacyjnych danych osobowych zgodnie z art. 76 rozporządzenia (UE) 2018/1725. W przypadku gdy takie inne dane dotyczą świadków lub pokrzywdzonych w rozumieniu ust. 2 niniejszego artykułu, decyzja o przetwarzaniu danych podejmowana jest przez zainteresowanych przedstawicieli krajowych.”;

b) dodaje się ustęp w brzmieniu:

„5. W przypadku gdy operacyjne dane osobowe przekazuje się zgodnie z art. 21a, Eurojust może przetwarzać wymienione w załączniku III operacyjne dane osobowe następujących osób:

a) osób, w odniesieniu do których, zgodnie z prawem krajowym zainteresowanego państwa członkowskiego, istnieją poważne powody, by podejrzewać, że popełniły lub popełnią przestępstwo, w przypadku którego Eurojust jest właściwy;

b) osób, które zostały skazane za popełnienie takiego przestępstwa.

Eurojust może nadal przetwarzać operacyjne dane osobowe, o których mowa w akapicie pierwszym lit. a), także po zakończeniu postępowania na podstawie prawa krajowego danego państwa członkowskiego nawet w przypadku uniewinnienia lub ostatecznej decyzji o odmowie ścigania – chyba że właściwy organ krajowy zdecyduje inaczej, indywidualnie dla każdego przypadku. W przypadku gdy postępowanie nie zakończyło się wyrokiem skazującym, przetwarzanie operacyjnych danych osobowych odbywa się wyłącznie w celu zidentyfikowania powiązań między toczącymi się, przyszłymi lub zakończonymi postępowaniami przygotowawczymi oraz wnoszonymi i popieranymi oskarżeniami, o których mowa w art. 23 ust. 2 lit. c).”;

8) w art. 29 wprowadza się następujące zmiany:

a) dodaje się ustęp w brzmieniu:

„1a. Eurojust nie przechowuje operacyjnych danych osobowych przekazanych zgodnie z art. 21a po tym spośród poniższych terminów, który nastąpi najwcześniej w:

a) terminie, w którym upłynął okres przedawnienia ścigania we wszystkich państwach członkowskich, których dotyczą postępowanie przygotowawcze lub wniesienie i popieranie oskarżenia;

b) terminie pięciu lat od dnia, w którym orzeczenie sądowe ostatniego z państw członkowskich, których dotyczą postępowanie przygotowawcze lub wniesienie i popieranie oskarżenia, stało się ostateczne lub terminie dwóch lat w przypadku uniewinnienia lub ostatecznej decyzji o odmowie ścigania;

c) terminie, w którym Eurojust został poinformowany o decyzji właściwego organu krajowego zgodnie z art. 27 ust. 5.";

b) ust. 2 i 3 otrzymują brzmienie:

„2. Przestrzeganie terminów przechowywania, o których mowa w ust. 1 i 1a, jest stale sprawdzane przez Eurojust przy pomocy właściwych środków automatycznego przetwarzania, w szczególności od momentu, w którym Eurojust przestaje udzielać wsparcia.

Co trzy lata od wprowadzenia danych sprawdzana jest również celowość ich przechowywania.

Jeżeli operacyjne dane osobowe, o których mowa w art. 27 ust. 4, przechowywane są przez okres dłuższy niż pięć lat, informuje się o tym EIOD.

3. Przed upływem jednego z terminów przechowywania, o których mowa w ust. 1 i 1a, Eurojust sprawdza, czy i jak długo konieczne jest dalsze przechowywanie operacyjnych danych osobowych do celów wykonywania jego zadań.

Eurojust może zdecydować na zasadzie odstępstwa o przechowywaniu takich danych do czasu następnego sprawdzenia. Powody dalszego przechowywania należy uzasadnić i odnotować. Jeżeli w momencie sprawdzenia nie podjęto decyzji o dalszym przechowywaniu operacyjnych danych osobowych, dane te są automatycznie usuwane.”;

9) dodaje się artykuł w brzmieniu:

„*Artykuł 54a*
Prokuratorzy łącznikowi z państw trzecich

1. Prokurator łącznikowy z państwa trzeciego może zostać oddelegowany do Eurojustu na podstawie umowy o współpracy zawartej przed dniem 12 grudnia 2019 r. między Eurojustem a danym państwem trzecim lub umowy międzynarodowej zawartej między Unią a państwem trzecim na podstawie art. 218 TFUE, umożliwiającej delegowanie prokuratora łącznikowego.

2. Prawa i obowiązki prokuratora łącznikowego określa się w umowie o współpracy lub umowie międzynarodowej, o których mowa w ust. 1, lub w porozumieniu roboczym zawartym zgodnie z art. 47 ust. 3.

3. Prokuratorom łącznikowym oddelegowanym do Eurojustu zapewnia się dostęp do zautomatyzowanego systemu zarządzania sprawami w celu umożliwienia bezpiecznej wymiany danych. Zgodnie z art. 45 i 46 Eurojust odpowiada za przetwarzanie danych osobowych przez prokuratorów łącznikowych w zautomatyzowanym systemie zarządzania sprawami.

Przekazywanie operacyjnych danych osobowych prokuratorom łącznikowym z państw trzecich za pośrednictwem zautomatyzowanego systemu zarządzania sprawami może odbywać się wyłącznie na zasadach i warunkach określonych w niniejszym rozporządzeniu, w umowie z danym państwem lub w innych mających zastosowanie instrumentach prawnych.

Art. 24 ust. 1 akapit drugi i art. 24 ust. 2 stosuje się odpowiednio do prokuratorów łącznikowych.

Kolegium określa szczegółowe warunki dostępu.”;

10) w art. 80 dodaje się następujące ustępy:

„9. Eurojust może nadal korzystać z zautomatyzowanego systemu zarządzania sprawami składającego się z akt tymczasowych i indeksu do dnia … [pierwszego dnia miesiąca następującego po upływie dwóch lat od daty wejścia w życie niniejszego rozporządzenia], o ile do tego czasu nie zostanie wprowadzony nowy zautomatyzowany system zarządzania sprawami.

10. Właściwe organy krajowe i Eurojust mogą nadal korzystać z innych kanałów komunikacji niż kanały, o których mowa w art. 22a ust. 1, do pierwszego dnia miesiąca następującego po upływie dwóch lat od daty wejścia w życie aktu wykonawczego, o którym mowa w art. 22b niniejszego rozporządzenia, o ile do tego czasu nie będą dostępne kanały komunikacji umożliwiające im bezpośrednią wymianę, o których mowa w art. 22a ust. 1.

11. Właściwe organy krajowe mogą nadal przekazywać informacje w sposób inny niż półautomatycznie zgodnie z art. 22a ust. 3 do pierwszego dnia miesiąca następującego po upływie dwóch lat od daty wejścia w życie aktu wykonawczego, o którym mowa w art. 22b niniejszego rozporządzenia, o ile do tego czasu nie zostaną ustanowione wymogi techniczne.”;

11) dodaje się załącznik w brzmieniu:

„Załącznik III:

a) informacje umożliwiające identyfikację osoby podejrzanej, oskarżonej, skazanej lub uniewinnionej:

Dotyczące osoby fizycznej:

– nazwisko;

– imiona;

– wszelkie pseudonimy;

– data urodzenia;

– miejsce urodzenia (miejscowość i państwo);

– obywatelstwo lub obywatelstwa;

– dowód tożsamości (rodzaj i numer dokumentu);

– płeć;

– miejsce zamieszkania;

Dotyczące osoby prawnej:

– nazwa przedsiębiorstwa;

– forma prawna;

– siedziba;

Dotyczące osoby fizycznej i prawnej:

– numery telefonów;

– adresy e-mail;

– dane rachunków bankowych lub rachunków w innych instytucjach finansowych;

b) informacje na temat przestępstwa terrorystycznego:

– informacje na temat osób prawnych uczestniczących w przygotowaniu lub popełnieniu przestępstwa terrorystycznego;

– kwalifikacja prawna przestępstwa zgodnie z prawem krajowym;

– stosowna forma poważnej przestępczości według wykazu, o którym mowa w załączniku I;

– przynależność do grupy terrorystycznej;

– rodzaj terroryzmu, np. dżihadystyczny, separatystyczny, lewicowy lub prawicowy;

– krótkie streszczenie sprawy;

c) informacje na temat postępowania krajowego:

– status takiego postępowania;

– właściwa prokuratura;

– sygnatura;

– data wszczęcia formalne postępowania sądowego;

– powiązania z innymi odpowiednimi sprawami;

d) dodatkowe informacje umożliwiające identyfikację osoby podejrzanej:

– dane daktyloskopijne pobrane zgodnie z prawem krajowym w ramach postępowania karnego;

– fotografie.”.

Artykuł 2

Zmiany w decyzji 2005/671/WSiSW

W decyzji 2005/671/WSiSW wprowadza się następujące zmiany:

1) w art. 1 uchyla się lit. c);

2) w art. 2 wprowadza się następujące zmiany:

a) uchyla się ust. 2;

b) ust. 3 otrzymuje brzmienie:

„3. Każde Państwo Członkowskie podejmuje niezbędne środki w celu zapewnienia, że przynajmniej informacje, o których mowa w ust. 4, dotyczące dochodzeń w sprawach przestępstw terrorystycznych, które mają lub mogą mieć wpływ na dwa lub więcej Państw Członkowskich, gromadzone przez właściwe organy, są przekazywane do Europolu zgodnie z prawem krajowym i rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794[*].

---

[*] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).”;

c) uchyla się ust. 5.

Artykuł 3

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w …

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący / Przewodnicząca*