

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2447**z dnia 4 grudnia 2025 r.****ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1727 w odniesieniu do specyfikacji i środków technicznych i innych wymogów dotyczących utworzenia i użytkowania zdecentralizowanego systemu informatycznego na potrzeby bezpiecznego przetwarzania i przekazywania informacji**

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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⁽¹⁾, w szczególności jego art. 22a ust. 3 i art. 22b ust. 1 lit. a), b), c) i d),

a także mając na uwadze, co następuje:

- (1) W rozporządzeniu (UE) 2018/1727 określono ramy nowej wewnętrznej cyfrowej infrastruktury Eurojustu oraz ustanowienia zdecentralizowanego systemu bezpiecznej komunikacji cyfrowej między właściwymi organami krajowymi państw członkowskich a Eurojustem.
- (2) Bezpieczna komunikacja cyfrowa ma się odbywać się za pośrednictwem zdecentralizowanego systemu informatycznego. W celu ustanowienia zdecentralizowanego systemu informatycznego należy określić specyfikacje techniczne określające metody komunikacji i specyfikacje techniczne protokołów komunikacyjnych, środki techniczne zapewniające minimalne normy bezpieczeństwa informacji i minimalne cele związane z dostępnością na potrzeby wdrożenia tego systemu.
- (3) Zgodnie z art. 22a ust. 1 rozporządzenia (UE) 2018/1727 zdecentralizowany system informatyczny ma obejmować systemy informatyczne państw członkowskich i Eurojustu oraz interoperacyjne punkty dostępu e-CODEX zapewniające wzajemne połączenia tych systemów informatycznych. Ramy te należy uwzględnić w specyfikacjach technicznych i innych wymogach dotyczących zdecentralizowanego systemu informatycznego określonych w niniejszym rozporządzeniu.
- (4) Punkty dostępu do zdecentralizowanego systemu informatycznego powinny opierać się na zatwierdzonych punktach dostępu e-CODEX zdefiniowanych w art. 3 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/850⁽²⁾.
- (5) Zdecentralizowany system informatyczny jest wdrażany w ramach większego zdecentralizowanego systemu informatycznego opartego na e-CODEX – określonego jako system wymiany cyfrowej wymiaru sprawiedliwości (ang. *Justice Digital Exchange System*, JUDEX). W związku należy zagwarantować skuteczną wymianę informacji na temat zmian o wymiarze horyzontalnym.
- (6) Zgodnie z art. 22a ust. 4 rozporządzenia (UE) 2018/1727 państwa członkowskie i Eurojust mogą w miejsce swoich krajowych systemów informatycznych wybrać oprogramowanie wzorcowe opracowane przez Komisję jako swój system *back-end*. Aby zagwarantowana była interoperacyjność, krajowe systemy informatyczne i oprogramowanie wzorcowe powinny podlegać tym samym specyfikacjom i wymogom technicznym.
- (7) Dane dotyczące przestępstw terrorystycznych i poważnej przestępczości zorganizowanej powinny być przekazywane w sposób ustrukturyzowany, co pozwoli poprawić jakość i przydatność informacji oraz zapewnić, aby informacje te mogły być skuteczniej wykorzystywane przez system zarządzania sprawami Eurojustu i aby kontrola krzyżowa z informacjami już przechowywanymi w tym systemie była efektywniejsza. Należy określić format i standardy techniczne przekazywania danych daktyloskopijnych i fotografii, które mogą być przekazywane Eurojustowi w celu identyfikacji osób, wobec których toczy się postępowanie karne związane z przestępstwami terrorystycznymi.

⁽¹⁾ Dz.U. L 295 z 21.11.2018, s. 138, ELI: <http://data.europa.eu/eli/reg/2018/1727/oj>.⁽²⁾ 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, ELI: <http://data.europa.eu/eli/reg/2022/850/oj>).

- (8) Eurojust ułatwia i wspiera wydawanie i wykonywanie wniosków dotyczących współpracy wymiarów sprawiedliwości, w tym wniosków i decyzji opartych na instrumentach służących wdrożeniu zasady wzajemnego uznawania. Właściwe organy krajowe powinny mieć możliwość zwracania się za pośrednictwem zdecentralizowanego systemu informatycznego do Eurojustu o pomoc i zapewnienie koordynacji.
- (9) Aby zapewnić efektywność i spójność, ważne jest, aby specyfikacje techniczne, które mają zostać ustanowione na podstawie rozporządzenia (UE) 2018/1727, były zgodne ze specyfikacjami technicznymi ustanowionymi na podstawie rozporządzeń Parlamentu Europejskiego i Rady (UE) 2023/2844 ⁽³⁾, (UE) 2023/1543 ⁽⁴⁾ i (UE) 2024/3011 ⁽⁵⁾, a także z przyszłymi środkami w zakresie cyfryzacji istotnymi dla mandatu Eurojustu w zakresie wspierania właściwych organów krajowych.
- (10) Zdecentralizowany system powinien umożliwiać Eurojustowi i organom prowadzenie wszelkich innych form komunikacji, np. przekazywanie, zgodnie z art. 22 rozporządzenia (UE) 2018/1727, informacji na temat wyników przetwarzania informacji, w tym istniejących powiązań ze sprawami już zarejestrowanymi w zautomatyzowanym systemie zarządzania sprawami, gdy Eurojust działa z własnej inicjatywy, lub informacji przekazywanych Eurojustowi w celu zabezpieczenia, analizowania i przechowywania dowodów związanych z ludobójstwem, zbrodniami przeciwko ludzkości, zbrodniami wojennymi i powiązanymi przestępstwami, zgodnie z art. 4 ust. 1 lit. j) tego rozporządzenia.
- (11) W celu zapewnienia, aby niniejsze rozporządzenie uwzględniało potrzeby operacyjne Eurojustu, przeprowadzono konsultacje z Eurojustem zgodnie z art. 22a ust. 3 rozporządzenia (UE) 2018/1727.
- (12) Zgodnie z art. 4 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Irlandia powiadomiła pismem z dnia 9 września 2019 r. o chęci przyjęcia rozporządzenia (UE) 2018/1727 oraz związania się jego przepisami. Uczestnictwo to potwierdzono w decyzji Komisji (UE) 2019/2006 ⁽⁶⁾. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/2131 ⁽⁷⁾ zmieniono rozporządzenie (UE) 2018/1727, aby umożliwić ustanowienie bezpiecznych kanałów komunikacji cyfrowej między Eurojustem a właściwymi organami krajowymi, oraz zapewniono podstawę prawną niniejszego rozporządzenia. W związku z tym, że Irlandia nie powiadomiła o chęci uczestniczenia w przyjęciu i stosowaniu rozporządzenia (UE) 2023/2131 ani nie powiadomiła o chęci przyjęcia tego rozporządzenia i związania się nim, Irlandia, zgodnie z art. 1, 2 i art. 4a ust. 1 protokołu nr 21, nie jest związana rozporządzeniem (UE) 2023/2131 ani go nie stosuje. W związku z powyższym Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia.
- (13) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczyła w przyjęciu rozporządzenia (UE) 2018/1727. Dania nie jest zatem związana niniejszym rozporządzeniem ani go nie stosuje.

⁽³⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2844 z dnia 13 grudnia 2023 r. w sprawie cyfryzacji współpracy sądowej i dostępu do wymiaru sprawiedliwości w sprawach cywilnych i handlowych o charakterze transgranicznym oraz współpracy wymiarów sprawiedliwości i dostępu do wymiaru sprawiedliwości w sprawach karnych o charakterze transgranicznym oraz zmieniające niektóre akty w tych dziedzinach (Dz.U. L, 2023/2844, 27.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2844/oj>).

⁽⁴⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L 191 z 28.7.2023, s. 118, ELI: <http://data.europa.eu/eli/reg/2023/1543/oj>).

⁽⁵⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/3011 z dnia 27 listopada 2024 r. w sprawie przekazywania postępowań w sprawach karnych (Dz.U. L, 2024/3011, 18.12.2024, ELI: <http://data.europa.eu/eli/reg/2024/3011/oj>).

⁽⁶⁾ Decyzja Komisji (UE) 2019/2006 z dnia 29 listopada 2019 r. dotycząca uczestnictwa Irlandii w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/1727 w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) (Dz.U. L 310 z 2.12.2019, s. 59, ELI: <http://data.europa.eu/eli/dec/2019/2006/oj>).

⁽⁷⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2131 z dnia 4 października 2023 r. 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 (Dz.U. L, 2023/2131, 11.10.2023, ELI: <http://data.europa.eu/eli/reg/2023/2131/oj>).

- (14) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 Parlamentu Europejskiego i Rady ⁽⁸⁾ skonsultowano się z Europejskim Inspektorem Ochrony Danych; swoją opinię wydał on w dniu 21 października 2025 r.,
- (15) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 22c rozporządzenia (UE) 2018/1727,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Specyfikacje techniczne dotyczące zdecentralizowanego systemu informatycznego

Specyfikacje techniczne, środki i cele zdecentralizowanego systemu informatycznego, o którym mowa w art. 22b ust. 1 lit. a), b), c) i d) rozporządzenia (UE) 2018/1727, określono w załączniku I do niniejszego rozporządzenia.

Artykuł 2

Cyfrowe standardy proceduralne

Cyfrowe standardy proceduralne mające zastosowanie do łączności elektronicznej za pośrednictwem zdecentralizowanego systemu informatycznego, o którym mowa w art. 22a ust. 3 rozporządzenia (UE) 2018/1727, określono w załączniku II do niniejszego rozporządzenia.

Artykuł 3

Specyfikacje techniczne dotyczące przekazywania odcisków palców i fotografii

Specyfikacje techniczne i format na potrzeby przekazywania odcisków palców i fotografii, o których to specyfikacjach i formacie mowa w art. 22a ust. 3 rozporządzenia (UE) 2018/1727, określono w załączniku III do niniejszego rozporządzenia.

Artykuł 4

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 Brukseli dnia 4 grudnia 2025 r.

W imieniu Komisji

Przewodnicząca

Ursula VON DER LEYEN

⁽⁸⁾ 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, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).

ZAŁĄCZNIK I

SPECYFIKACJE TECHNICZNE, ŚRODKI I CELE DOTYCZĄCE ZDECENTRALIZOWANEGO SYSTEMU TELEINFORMATYCZNEGO

1. Wprowadzenie i zakres

W niniejszym załączniku ustanowiono specyfikacje techniczne, środki i cele zdecentralizowanego systemu teleinformatycznego na potrzeby wymiany informacji prowadzonej na podstawie rozporządzenia (UE) 2018/1727.

Zdecentralizowany charakter systemu teleinformatycznego umożliwia bezpośrednią i bezpieczną wymianę danych między właściwymi organami krajowymi a Eurojustem.

2. Definicje

Do celów niniejszego załącznika stosuje się następujące definicje:

- 2.1. „Hypertext Transfer Protocol Secure” lub „HTTPS” oznacza szyfrowane kanały komunikacji i bezpiecznych połączeń;
- 2.2. „niezaprzeczalność pochodzenia” oznacza środki dostarczające dowodu integralności i pochodzenia danych metodami takimi jak certyfikacja cyfrowa, infrastruktura klucza publicznego, podpisy cyfrowe i pieczęcie elektroniczne;
- 2.3. „niezaprzeczalność odbioru” oznacza środki dostarczające inicjatorowi dowodu odbioru danych przez ich docelowego odbiorcę metodami takimi jak certyfikacja cyfrowa, infrastruktura klucza publicznego, podpisy cyfrowe i pieczęcie elektroniczne;
- 2.4. „SOAP” (Simple Object Access Protocol) oznacza, zgodnie z normami konsorcjum World Wide Web, specyfikację protokołu przesyłania komunikatów służącego do wymiany ustrukturyzowanych informacji w ramach wdrażania usług sieciowych w sieciach komputerowych;
- 2.5. „REST” (zmiana stanu poprzez reprezentacje, ang. Representational State Transfer) oznacza styl architektury oprogramowania służący do projektowania aplikacji sieciowych, oparty na bezstanowym modelu komunikacji klient-serwer, wykorzystujący standardowe metody wykonywania operacji na zasobach, które są zazwyczaj reprezentowane w ustrukturyzowanych formatach;
- 2.6. „usługa sieciowa” oznacza system oprogramowania służący do obsługi interoperacyjnej interakcji maszyna-maszyna w ramach sieci, posiadający interfejs opisany w formacie nadającym się do przetwarzania maszynowego;
- 2.7. „wymiana danych” oznacza wymianę komunikatów i dokumentów za pośrednictwem zdecentralizowanego systemu informatycznego;
- 2.8. „e-CODEX” oznacza system e-CODEX, o którym mowa w art. 3 ust. 1 rozporządzenia (UE) 2022/850;
- 2.9. „unijne słowniki podstawowe e-Justice” oznaczają unijne słowniki podstawowe e-Justice zdefiniowane w pkt 4 załącznika do rozporządzenia (UE) 2022/850;
- 2.10. „ebMS” (ang. „ebXML Messaging Service”) oznacza usługę przesyłania wiadomości ebXML – protokół przesyłania wiadomości opracowany w ramach OASIS, który umożliwia bezpieczną, niezawodną i interoperacyjną wymianę elektronicznych dokumentów biznesowych z wykorzystaniem SOAP. Ułatwia on integrację między przedsiębiorstwami korzystającymi z różnych systemów;
- 2.11. „AS4” stanowi skrót od ang. „Applicability Statement 4” i oznacza standard OASIS profilujący ebMS 3.0; upraszcza on bezpieczną i interoperacyjną komunikację między przedsiębiorstwami poprzez wykorzystanie otwartych standardów takich jak SOAP i WS-Security;

- 2.12. „zakładany czas wznowienia funkcjonowania” oznacza maksymalny akceptowalny czas przywrócenia działania usługi po incydencie;
- 2.13. „akceptowalny poziom utraty danych” oznacza maksymalną dopuszczalną wartość utraty danych w przypadku awarii.

3. **Metody komunikacji drogą elektroniczną**

- 3.1. Do wymiany wiadomości i dokumentów w ramach zdecentralizowanego systemu teleinformatycznego stosuje się metody łączności oparte na usługach, takie jak usługi sieciowe lub inne elementy wielokrotnego użytku i rozwiązania oprogramowania.
- 3.2. W szczególności w zdecentralizowanym systemie teleinformatycznym wykorzystuje się komunikację za pośrednictwem punktów dostępu e-CODEX, określonych w art. 5 ust. 2 rozporządzenia (UE) 2022/850. W związku z tym, aby zapewnić skuteczną oraz interoperacyjną transgraniczną wymianę danych, zdecentralizowany system teleinformatyczny musi umożliwiać komunikację w systemie e-CODEX.

4. **Protokoły komunikacyjne**

- 4.1. Zdecentralizowany system teleinformatyczny wykorzystuje bezpieczne protokoły internetowe do:
 - a) komunikacji w ramach zdecentralizowanego systemu teleinformatycznego między właściwymi organami a Eurojustem;
 - b) komunikacji z bazą danych właściwych organów/Trybunału, o której mowa w pkt 7.1.
- 4.2. Na potrzeby definiowania i przekazywania ustrukturyzowanych danych i metadanych elementy zdecentralizowanego systemu teleinformatycznego opierają się na kompleksowych i powszechnie przyjętych normach i protokołach branżowych, takich jak SOAP i REST.
- 4.3. W przypadku protokołów transportowych i protokołów przesyłania komunikatów zdecentralizowany system teleinformatyczny opiera się na bezpiecznych standardowych protokołach, takich jak:
 - a) profil AS4 na potrzeby transgranicznej wymiany danych, zapewniający bezpieczne i niezawodne przesyłanie komunikatów oraz szyfrowanie i niezaprzeczalność;
 - b) HTTPS/RESTful API do komunikacji obsługującej formaty JSON i XML;
 - c) SOAP do interakcji o wysokiej niezawodności, obejmujący WS-Security do celów uwierzytelniania i szyfrowania.
- 4.4. Na potrzeby sprawnej i interoperacyjnej wymiany danych protokoły komunikacyjne wykorzystywane przez zdecentralizowany system teleinformatyczny są zgodne z odpowiednimi normami interoperacyjności.
- 4.5. W stosownych przypadkach w schematach XML wykorzystuje się odpowiednie normy lub słowniki, które są niezbędne do właściwej walidacji elementów oraz typów określonych w danym schemacie. Te normy lub słowniki mogą obejmować:
 - a) unijny słownik podstawowy e-Justice;
 - b) niekwalifikowane typy danych;
 - c) listę kodów językowych Unii Europejskiej.
- 4.6. Jeśli chodzi o protokoły bezpieczeństwa i uwierzytelniania, zdecentralizowany system teleinformatyczny bazuje na opartych na standardach protokołach, takich jak:
 - a) TLS (ang. „Transport Layer Security” – „zabezpieczenia warstwy transportowej”) do szyfrowanej i uwierzytelnionej komunikacji w sieci, obsługujący wzajemne uwierzytelnianie certyfikatami cyfrowymi X.509;
 - b) OAuth/OpenID Connect (OIDC) na potrzeby bezpiecznego uwierzytelniania i autoryzacji;
 - c) PKI (ang. „public key infrastructure” – „infrastruktura klucza publicznego”) i digital signatures („podpisy cyfrowe”) na potrzeby bezpiecznej wymiany kluczy i weryfikacji integralności komunikatów, wykorzystujące certyfikaty cyfrowe (X.509) wydane przez zaufane organy certyfikacji.

5. Cele w zakresie bezpieczeństwa informacji oraz odpowiednie środki techniczne

- 5.1. W zakresie wymiany informacji za pośrednictwem zdecentralizowanego systemu teleinformatycznego środki techniczne zapewniające minimalne normy bezpieczeństwa technologii informacyjnych obejmują:
- a) środki zapewniające poufność informacji, w tym wykorzystanie bezpiecznych kanałów komunikacji;
 - b) środki zapewniające integralność danych podczas ich przechowywania i przesyłania;
 - c) środki zapewniające niezaprzeczalność pochodzenia nadawcy informacji w ramach zdecentralizowanego systemu teleinformatycznego i niezaprzeczalność odbioru informacji;
 - d) środki zapewniające rejestrowanie zdarzeń związanych z bezpieczeństwem informacji zgodnie z uznanymi międzynarodowymi zaleceniami dotyczącymi norm bezpieczeństwa technologii informacyjnych⁽¹⁾;
 - e) środki zapewniające uwierzytelnianie i upoważnianie użytkownika oraz środki weryfikacji tożsamości systemów podłączonych do zdecentralizowanego systemu teleinformatycznego.
- 5.2. Elementy zdecentralizowanego systemu teleinformatycznego zapewniają bezpieczną komunikację i transmisję danych poprzez szyfrowanie, infrastrukturę klucza publicznego z certyfikatami cyfrowymi na potrzeby uwierzytelniania i bezpiecznej wymiany kluczy oraz bezpieczne protokoły przesyłania wiadomości, takie jak AS4 (ebMS), RESTful API i SOAP w celu zachowania poufności i integralności wiadomości.
- 5.3. W przypadku gdy w kontekście zdecentralizowanego systemu teleinformatycznego wykorzystuje się protokół TLS, stosuje się najnowszą stabilną wersję protokołu lub, w przypadku jej braku, wersję bez znanych luk w zabezpieczeniach. Dozwolone są wyłącznie klucze o długości zapewniającej odpowiedni poziom bezpieczeństwa kryptograficznego, nie mogą być natomiast stosowane zestawy szyfrów, o których wiadomo, że są niepełne lub przestarzałe.
- 5.4. W miarę możliwości certyfikaty cyfrowe PKI używane do celów funkcjonowania zdecentralizowanego systemu teleinformatycznego są wydawane przez organy certyfikacji uznane za kwalifikowanych dostawców usług zaufania zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014⁽²⁾. Wdraża się środki zapewniające, aby takich certyfikatów używano wyłącznie zgodnie z przeznaczeniem, na wymaganym poziomie zaufania i zgodnie z mającymi zastosowanie wymogami rozporządzenia (UE) nr 910/2014.
- 5.5. Elementy zdecentralizowanego systemu teleinformatycznego opracowuje się zgodnie z zasadą uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych oraz wdraża się odpowiednie środki administracyjne, organizacyjne i techniczne w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa.
- 5.6. Komisja projektuje, opracowuje i utrzymuje oprogramowanie wzorcowe zgodnie z wymogami i zasadami ochrony danych określonymi w rozporządzeniu (UE) 2018/1725. Oprogramowanie wzorcowe dostarczone przez Komisję umożliwia państwom członkowskim wykonywanie ich obowiązków zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679⁽³⁾ i dyrektywą (UE) 2016/680.

⁽¹⁾ Bez uszczerbku dla rejestrowania do celów bezpieczeństwa mechanizmy rejestrowania wykorzystywane przez elementy zdecentralizowanego systemu teleinformatycznego umożliwiają, w stosownych przypadkach, zapewnienie zgodności z wymogami określonymi w art. 88 rozporządzenia (UE) 2018/1725 oraz, w stosownych przypadkach, w art. 25 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSISW (Dz.U. L 119 z 4.5.2016, s. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>).

⁽²⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchyłające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

⁽³⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

- 5.7. Państwa członkowskie, które korzystają z krajowego systemu back-end innego niż oprogramowanie wzorcowe, wdrażają niezbędne środki w celu zapewnienia zgodności swojego krajowego systemu back-end z wymogami odpowiednio rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680.
- 5.8. Eurojust wdraża niezbędne środki w celu zapewnienia zgodności swojego systemu back-end lub używanej przez siebie instancji oprogramowania wzorcowego z wymogami rozporządzeń (UE) 2018/1725 i (UE) 2018/1727.
- 5.9. W odniesieniu do stanowiących część zdecentralizowanego systemu teleinformatycznego systemów informatycznych, za które odpowiadają państwa członkowskie i Eurojust, podmioty te ustanawiają solidne mechanizmy wykrywania zagrożeń i reagowania na incydenty w celu zapewnienia terminowego wykrywania incydentów bezpieczeństwa, łagodzenia ich skutków i przywracania funkcjonowania systemu po incydencie, zgodnie ze swoimi odpowiednimi politykami.

6. **Minimalne cele związane z dostępnością**

- 6.1. Eurojust i państwa członkowskie zapewniają przez całą dobę, 7 dni w tygodniu dostępność elementów zdecentralizowanego systemu teleinformatycznego, za które odpowiadają, przy docelowym wskaźniku dostępności technicznej wynoszącym co najmniej 98 % w ujęciu rocznym, z wyłączeniem planowych prac konserwacyjnych.
- 6.2. Komisja zapewnia przez całą dobę, 7 dni w tygodniu dostępność bazy danych Trybunału, przy docelowym wskaźniku dostępności technicznej wynoszącym ponad 99 % rocznie, z wyłączeniem planowych prac konserwacyjnych.
- 6.3. W miarę możliwości w dni robocze prace konserwacyjne planuje się w godz. 20.00–7.00 czasu środkowoeuropejskiego.
- 6.4. Państwa członkowskie powiadamiają Komisję, Eurojust i pozostałe państwa członkowskie o pracach konserwacyjnych w następujący sposób:
- a) z wyprzedzeniem 5 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres do 4 godzin;
 - b) z wyprzedzeniem 10 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres od 4 do 12 godzin;
 - c) z wyprzedzeniem 30 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres dłuższy niż 12 godzin.
- 6.5. W przypadku gdy państwa członkowskie mają stałe i regularne okna czasowe wykonywania prac konserwacyjnych, informują one Komisję, Eurojust i pozostałe państwa członkowskie o datach i godzinach takich stałych i regularnych okien czasowych prac konserwacyjnych. Na zasadzie odstępstwa od obowiązków określonych w zdaniu pierwszym, jeżeli elementy zdecentralizowanego systemu teleinformatycznego, za które odpowiadają państwa członkowskie, staną się niedostępne w takim stałym regularnym oknie czasowym, państwa członkowskie mogą zdecydować o niepowiadamianiu Komisji o każdym takim przypadku.

- 6.6. W przypadku nieoczekiwanej awarii technicznej elementu zdecentralizowanego systemu teleinformatycznego, za który odpowiedzialne są państwa członkowskie, państwa członkowskie niezwłocznie informują Komisję i pozostałe państwa członkowskie o awarii oraz, o ile jest on znany, o przewidywanym terminie wznowienia funkcjonowania danego elementu systemu.
- 6.7. Eurojust powiadamia Komisję i państwa członkowskie o pracach konserwacyjnych w następujący sposób:
- a) z wyprzedzeniem 5 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres do 4 godzin;
 - b) z wyprzedzeniem 10 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres od 4 do 12 godzin;
 - c) z wyprzedzeniem 30 dni roboczych, jeśli prace mogą spowodować brak dostępu przez okres dłuższy niż 12 godzin.
- 6.8. W przypadku gdy Eurojust ma stałe i regularne okna czasowe wykonywania prac konserwacyjnych, Eurojust informuje Komisję i pozostałe państwa członkowskie o datach i godzinach takich stałych i regularnych okien czasowych prac konserwacyjnych. Na zasadzie odstępstwa od obowiązków określonych w zdaniu pierwszym, jeżeli elementy zdecentralizowanego systemu teleinformatycznego, za które odpowiada Eurojust, staną się niedostępne w takim stałym regularnym oknie czasowym, Eurojust może zdecydować o niepowiadamianiu Komisji o każdym takim przypadku.
- 6.9. W przypadku nieoczekiwanej awarii technicznej elementu zdecentralizowanego systemu teleinformatycznego, za który odpowiedzialny jest Eurojust, niezwłocznie informuje on Komisję i państwa członkowskie o awarii oraz, o ile jest znany, o przewidywanym terminie wznowienia funkcjonowania danego elementu systemu.
- 6.10. W przypadku nieoczekiwanej awarii technicznej bazy danych właściwych organów/Trybunału Komisja niezwłocznie informuje Eurojust i państwa członkowskie o braku dostępu oraz, o ile jest on znany, o przewidywanym terminie wznowienia funkcjonowania bazy danych.
- 6.11. W przypadku zakłóceń w świadczeniu usług państwa członkowskie i Eurojust zapewniają szybkie przywrócenie usługi i minimalną utratę danych, zgodnie z zakładanym okresem wznowienia funkcjonowania oraz z akceptowalnym poziomem utraty danych.
- 6.12. Państwa członkowskie i Eurojust wdrażają odpowiednie środki w celu zrealizowania założeń, o których mowa powyżej, oraz ustanawiają procedury skutecznego reagowania na incydenty.

7. Właściwe organy/baza danych Trybunału (CDB)

- 7.1. Zgodnie z art. 22a rozporządzenia (UE) 2018/1727 komunikację elektroniczną między właściwymi organami krajowymi a Eurojustem umożliwia zdecentralizowany system teleinformatyczny. Biorąc pod uwagę obowiązki w zakresie wymiany informacji między właściwymi organami krajowymi a Eurojustem wynikające z art. 21, 21a i 22, ale także rolę Eurojustu dotyczącą ułatwiania i wspierania w odniesieniu do wydawania i wykonywania wniosków o wzajemną pomoc prawną lub o wzajemne uznanie zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2018/1727, podczas korzystania ze zdecentralizowanego systemu teleinformatycznego zaangażowane właściwe organy muszą być łatwe do zidentyfikowania. W związku z tym do celów zdecentralizowanego systemu teleinformatycznego konieczne jest utworzenie wiarygodnej bazy danych zawierającej informacje dotyczące tych organów.

- 7.2. CDB zawiera następujące informacje w ustrukturyzowanym formacie:
- a) do celów art. 8 ust. 1, 3 i 4, art. 21, 21a i 22 rozporządzenia (UE) 2018/1727 informacje na temat właściwych organów krajowych, w tym korespondentów krajowych, o których mowa w art. 20 tego rozporządzenia, a także przedstawicieli krajowych zgodnie z art. 7 ⁽⁴⁾ tego rozporządzenia;
 - b) w stosownych przypadkach informacje niezbędne do określenia geograficznych lub merytorycznych obszarów kompetencji właściwych organów lub inne istotne kryteria niezbędne do ustalenia ich właściwości;
 - c) informacje niezbędne do prawidłowego routingu wiadomości technicznych w ramach zdecentralizowanego systemu teleinformatycznego.
- 7.3. Komisja jest odpowiedzialna za opracowanie, utrzymanie, obsługę i wspieranie funkcjonowania CDB;
- 7.4. CDB umożliwia państwom członkowskim i Eurojustowi aktualizowanie zawartych w niej informacji, a właściwym organom krajowym i przedstawicielom krajowym uczestniczącym w zdecentralizowanym systemie teleinformatycznym – programowy dostęp do tych informacji i ich pobieranie;
- 7.5. dostęp do CDB jest możliwy za pośrednictwem wspólnego protokołu komunikacyjnego, niezależnie od tego, czy właściwe organy podłączone do zdecentralizowanego systemu teleinformatycznego korzystają z krajowego systemu back-end, czy też wdrażają oprogramowanie wzorcowe;
- 7.6. państwa członkowskie zapewniają, aby zawarte w CDB informacje dotyczące ich właściwych organów określone w pkt 7.2 były kompletne, dokładne i aktualne.
-

⁽⁴⁾ Pozostaje to bez uszczerbku dla przekazania przez przedstawiciela krajowego uprawnień na rzecz zastępcy, innych pracowników biura krajowego lub upoważnionych pracowników Eurojustu.

ZAŁĄCZNIK II

CYFROWE STANDARDY PROCEDURALNE

W art. 3 pkt 9 rozporządzenia (UE) 2022/850 zdefiniowano cyfrowe standardy proceduralne jako specyfikacje techniczne dla modeli procesów biznesowych i schematów danych określające elektroniczną strukturę danych wymienianych za pośrednictwem systemu e-CODEX.

W niniejszym załączniku określono specyfikacje techniczne dla modeli procesów biznesowych oraz specyfikacje techniczne schematów danych.

1. Specyfikacje techniczne dla modeli procesów biznesowych na podstawie rozporządzenia (UE) 2018/1727

Specyfikacje techniczne dla modeli procesów biznesowych określono w pkt 1.1–1.5. Określono w nich kluczowe aspekty niezbędne, aby umożliwić komunikację elektroniczną do celów rozporządzenia (UE) 2018/1727 za pośrednictwem zdecentralizowanego systemu teleinformatycznego.

Zdecentralizowany system teleinformatyczny umożliwia wymianę informacji wyłącznie między właściwymi organami krajowymi państwa członkowskiego a przedstawicielem krajowym z tego państwa członkowskiego.

1.1. Wymiana informacji dotycząca europejskiego sądowego rejestru antyterrorystycznego – art. 21a rozporządzenia (UE) 2018/1727

1.1.1. Model przekazania danych do europejskiego sądowego rejestru antyterrorystycznego:

Właściwy organ krajowy przekazuje przedstawicielowi krajowemu dane dotyczące postępowań w sprawie terroryzmu przeznaczone do europejskiego sądowego rejestru antyterrorystycznego.

1.1.2. Model odbioru danych z europejskiego sądowego rejestru antyterrorystycznego:

Przedstawiciel krajowy otrzymuje dane z europejskiego sądowego rejestru antyterrorystycznego.

1.1.3. Model wniosku o zgodę:

Przedstawiciel krajowy zwraca się o zgodę do swojego właściwego organu krajowego.

1.1.4. Model odbioru wniosku o zgodę:

Właściwy organ krajowy otrzymuje wniosek o zgodę.

1.1.5. Model wysłania odpowiedzi na wniosek o zgodę:

Właściwy organ krajowy wysyła odpowiedź na wniosek o zgodę.

1.1.6. Model odbioru odpowiedzi na wniosek o zgodę:

Przedstawiciel krajowy otrzymuje odpowiedź na wniosek o zgodę.

1.1.7. Model informacji o powiązaniu:

Przedstawiciel krajowy informuje właściwy organ krajowy o powiązaniu z inną sprawą.

1.1.8. Model aktualizacji danych w europejskim sądowym rejestrze antyterrorystycznym:

Właściwy organ krajowy przekazuje swojemu przedstawicielowi krajowemu dane, które wymagają aktualizacji lub usunięcia.

1.1.9. Model odbioru zaktualizowanych danych z europejskiego sądowego rejestru antyterrorystycznego:

Przedstawiciel krajowy otrzymuje dane z europejskiego sądowego rejestru antyterrorystycznego, które wymagają aktualizacji lub usunięcia.

- 1.2. *Wymiana informacji dotyczących poważnej przestępczości – art. 21 rozporządzenia (UE) 2018/1727*
- 1.2.1. Model przekazania danych dotyczących poważnej przestępczości transgranicznej:
Właściwy organ krajowy przekazuje Eurojustowi dane dotyczące poważnej przestępczości transgranicznej.
- 1.2.2. Model odbioru danych dotyczących poważnej przestępczości transgranicznej:
Przedstawiciel krajowy otrzymuje dane dotyczące poważnej przestępczości transgranicznej.
- 1.2.3. Model wniosku o zgodę:
Przedstawiciel krajowy zwraca się o zgodę do swojego właściwego organu krajowego.
- 1.2.4. Model odbioru wniosku o zgodę:
Właściwy organ krajowy otrzymuje wniosek o zgodę.
- 1.2.5. Model wysłania odpowiedzi na wniosek o zgodę:
Właściwy organ krajowy wysyła odpowiedź na wniosek o zgodę.
- 1.2.6. Model odbioru odpowiedzi na wniosek o zgodę:
Przedstawiciel krajowy otrzymuje odpowiedź na wniosek o zgodę.
- 1.2.7. Model informacji o powiązaniu:
Przedstawiciel krajowy informuje właściwy organ krajowy o powiązaniu z inną sprawą.
- 1.2.8. Model aktualizacji danych dotyczących poważnej przestępczości transgranicznej:
Właściwy organ krajowy przekazuje swojemu przedstawicielowi krajowemu dane, które wymagają aktualizacji lub usunięcia.
- 1.2.9. Model odbioru zaktualizowanych danych dotyczących poważnej przestępczości transgranicznej:
Przedstawiciel krajowy otrzymuje dane dotyczące poważnej przestępczości transgranicznej, które wymagają aktualizacji lub usunięcia.
- 1.3. *Wymiana informacji ogólnych*
- 1.3.1. Model wysłania informacji:
Przedstawiciel krajowy wysyła informacje właściwemu organowi krajowemu lub odwrotnie.
- 1.3.2. Model odbioru informacji:
Właściwy organ krajowy lub przedstawiciel krajowy otrzymuje informacje.
- 1.3.3. Model odpowiedzi na informacje:
Właściwy organ krajowy odpowiada na informacje otrzymane od przedstawiciela krajowego lub odwrotnie.
- 1.3.4. Model odbioru odpowiedzi:
Przedstawiciel krajowy otrzymuje odpowiedź od właściwego organu krajowego.

1.3.5. Model wysłania informacji:

Właściwy organ krajowy wysyła informacje przedstawicielowi krajowemu.

1.3.6. Model odbioru informacji:

Przedstawiciel krajowy otrzymuje informacje.

1.3.7. Model odpowiedzi na informacje:

Przedstawiciel krajowy odpowiada na informacje otrzymane od właściwego organu krajowego.

1.3.8. Model odbioru odpowiedzi:

Właściwy organ krajowy otrzymuje odpowiedź od przedstawiciela krajowego.

1.4. *Ułatwienie i wsparcie – art. 8 ust. 1 rozporządzenia (UE) 2018/1727*

Uwaga: W przypadku gdy modele ułatwienia i wsparcia określone w pkt 1.5 obejmują wymianę przepisowych formatów ustanowionych aktami prawnymi Unii w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych, w modelach tych wykorzystuje się, o ile są dostępne, odpowiednie uporządkowane przedstawienia danych i schematy XML opracowane do celów tych aktów, na przykład ustanowione do celów rozporządzenia wykonawczego (UE) 2023/2844 lub innych odpowiednich instrumentów.

1.5. *Model wniosku o ułatwienie lub wsparcie:*

1.5.1. Model przekazania wniosku o ułatwienie lub wsparcie:

Właściwy organ krajowy przekazuje wniosek o ułatwienie lub wniosek o wsparcie swojemu przedstawicielowi krajowemu.

1.5.2. Model odbioru wniosku o ułatwienie lub wsparcie:

Przedstawiciel krajowy otrzymuje wniosek o ułatwienie lub wsparcie i przekazuje go dalej przedstawicielowi krajowemu państwa członkowskiego, do którego skierowano wniosek, poza systemem JUDEX.

1.5.3. Model przekazania dalej wniosku o ułatwienie lub wsparcie do właściwego organu krajowego:

Przedstawiciel krajowy państwa członkowskiego, do którego skierowano wniosek, wysyła wniosek do swojego właściwego organu krajowego.

1.5.4. Model odbioru wniosku o ułatwienie lub wsparcie:

Właściwy organ krajowy otrzymuje wniosek o ułatwienie lub wsparcie.

1.5.5. Model wysłania odpowiedzi na wniosek o ułatwienie lub wsparcie:

Właściwy organ krajowy wysyła odpowiedź na wniosek lub informacje dotyczące wniosku przedstawicielowi krajowemu państwa członkowskiego, do którego skierowano wniosek.

1.5.6. Model odbioru odpowiedzi na wniosek o ułatwienie lub wsparcie:

Przedstawiciel krajowy otrzymuje od właściwego organu krajowego odpowiedź na wniosek lub informacje dotyczące wniosku o ułatwienie lub wsparcie i udostępnia je przedstawicielowi krajowemu wnioskującego państwa członkowskiego poza systemem JUDEX.

1.5.7. Model odpowiedzi na wniosek o ułatwienie lub wsparcie:

Przedstawiciel krajowy wnioskującego państwa członkowskiego odpowiada na informacje dotyczące wniosku właściwego organu krajowego o ułatwienie lub wsparcie.

1.5.8. Model odbioru odpowiedzi:

Właściwy organ krajowy otrzymuje odpowiedź lub informacje dotyczące wniosku o ułatwienie lub wsparcie.

2. Specyfikacje techniczne schematów danych

Specyfikacje techniczne, które mają służyć jako podstawa do opracowania definicji schematów XML (XSD) na potrzeby cyfryzacji zgodnie z rozporządzeniem (UE) 2018/1727, określono w pkt 2.1 i 2.2 niniejszego załącznika. W specyfikacjach tych zdefiniowano kluczowe elementy i wszelkie inne informacje w celu zapewnienia wyczerpującego opisu na potrzeby opracowania tych schematów.

Opis ma mieć charakter ogólny, umożliwiający modyfikację i rozszerzenie opracowanych schematów XSD bez konieczności wprowadzania istotnych zmian w tych specyfikacjach.

Specyfikacje mają zastosowanie do przepisowego formatu schematów załączonego do rozporządzenia (UE) 2018/1727, wszelkich uprzednio zdefiniowanych wiadomości lub dowolnych wiadomości tekstowych wykorzystywanych w wymianach danych na podstawie tego rozporządzenia.

2.1. Kwestie ogólne

W odniesieniu do wszystkich schematów, które należy przedstawić, stosuje się następujące przepisy:

2.1.1. Wersjonowanie

Podaje się atrybut wersji, który ułatwia zarządzanie wersjami schematu i umożliwia aktualizację schematu w przyszłych iteracjach odpowiednio do wymogów biznesowych. Przy wprowadzaniu nowych funkcji lub ulepszeń atrybut wersji wskazuje, czy nowa wersja jest kompatybilna wstecznie.

2.1.2. Deklaracja schematu i metadane

— W stosownych przypadkach w schemacie wykorzystuje się odpowiednie normy lub słowniki, wymagane przez system e-CODEX do zapewnienia interoperacyjności, które są niezbędne do właściwej walidacji elementów oraz typów określonych w danym schemacie. Składana dokumentacja może obejmować:

- unijny słownik podstawowy e-Justice
- niekwalifikowane typy danych
- listę kodów językowych Unii Europejskiej

— W stosownych przypadkach schemat może również zawierać odpowiednie normy ETSI w celu wykorzystania ich definicji.

2.1.3. Adnotacje i dokumentacja

— **Adnotacje:** Każdemu elementowi w schemacie zwykle towarzyszą adnotacje. W adnotacjach zawarte są czytelne dla człowieka informacje na temat danego elementu, często określające w jasny i zwięzły sposób jego przeznaczenie lub zastosowanie.

2.1.4. Użycie i możliwość dostosowania

Schemat jest zgodny z zasadami określonymi w lit. a)–d):

- a) **Struktura modułowa:** każdą sekcję projektuje się w sposób zapewniający określoną funkcjonalność, a także możliwe jest jej ponowne użycie lub niezależne dostosowanie. To ułatwia dostosowanie schematu do różnych przypadków użycia.
- b) **Możliwość rozszerzenia:** schemat projektuje się tak, aby umożliwić włączanie nowych elementów lub atrybutów, jeżeli w przyszłości potrzebne będą dodatkowe informacje. Osiąga się to poprzez zastosowanie opcjonalnych elementów i sekwencji, które można rozszerzać bez naruszania istniejących wdrożeń.

- c) **Struktura możliwa do dostosowania:** schemat projektuje się w sposób umożliwiający w razie potrzeby dodanie lub modyfikację elementów lub rodzajów danych. Struktura schematu umożliwia uwzględnienie zmian w wymogach bez potrzeby większych modyfikacji projektu.
- d) **Elementy opcjonalne:** elementy schematu mogą być oznaczone jako opcjonalne, tj. można je uwzględnić lub pomijać odpowiednio do konkretnych okoliczności.

Schemat projektuje się w taki sposób, aby umożliwić gromadzenie ustrukturyzowanych danych na potrzeby konkretnych wniosków.

2.1.5. Modyfikacje

Projekt schematu charakteryzuje się elastycznością, modułowością i łatwością dostosowania. Złożone typy i elementy opcjonalne włącza się do projektu w taki sposób, aby możliwe było jego użycie w różnych scenariuszach, a zarazem aby był łatwy do modyfikacji i rozszerzenia.

2.2. Wymiana danych ustrukturyzowanych

Dane ustrukturyzowane, o których mowa w pkt 2.2.1 i 2.2.2, udostępnia się zgodnie z art. 22a ust. 3 rozporządzenia (UE) 2018/1727. Schemat umożliwia również oznaczanie zbiorów danych, które mają zostać usunięte w przyszłych aktualizacjach.

2.2.1. Dane z europejskiego sądowego rejestru antyterrorystycznego

W poniższych specyfikacjach technicznych dotyczących schematu danych ustanawia się ustrukturyzowane ramy tworzenia schematu w formacie XML.

- a) Sekcja najwyższego poziomu
Ta sekcja najwyższego poziomu odpowiada informacjom określonym w załączniku III do rozporządzenia (UE) 2018/1727: informacje na potrzeby europejskiego sądowego rejestru antyterrorystycznego.
- b) Struktura wiadomości
Struktura danych z europejskiego sądowego rejestru antyterrorystycznego składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:
 - (i) informacje służące identyfikacji osób fizycznych:
 - nazwisko;
 - imiona;
 - wszelkie pseudonimy;
 - data urodzenia;
 - miejsce urodzenia (miejscowość i państwo);
 - obywatelstwo lub obywatelstwa;
 - dowód tożsamości (rodzaj i numer dokumentu);
 - płeć;
 - miejsce zamieszkania;
 - (ii) informacje służące identyfikacji osób prawnych:
 - nazwa przedsiębiorstwa;
 - forma prawna;
 - siedziba;

- (iii) informacje służące identyfikacji osób zarówno fizycznych, jak i prawnych:
 - numery telefonu;
 - adresy poczty elektronicznej;
 - dane rachunków bankowych lub rachunków w innych instytucjach finansowych;
 - status w postępowaniu;
- (iv) informacje na temat przestępstwa:
 - 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;
- (v) informacje na temat postępowania krajowego:
 - status takiego postępowania;
 - właściwa prokuratura;
 - numer sprawy;
 - data wszczęcia formalnego postępowania sądowego;
 - powiązania z innymi odpowiednimi sprawami;
- (vi) pole na dodatkowe informacje (dowolny tekst);
- (vii) kod uprzedniej zgody.

2.2.2. Dane przekazywane zgodnie z art. 21 rozporządzenia (UE) 2018/1727

- a) Art. 21 ust. 4 rozporządzenia (UE) 2018/1727 dotyczący utworzenia wspólnych zespołów dochodzeniowo-śledczych („zespołów JIT”)
 - (i) Sekcja najwyższego poziomu
Ta sekcja najwyższego poziomu odpowiada informacjom określonym w art. 21 ust. 4 rozporządzenia (UE) 2018/1727: informacje na temat tworzenia zespołów JIT.
 - (ii) Struktura wiadomości
Struktura danych składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:
 - Krajowy organ sądowy odpowiedzialny za postępowanie karne
 - Krajowy numer referencyjny postępowania karnego
 - Status postępowania karnego
 - Przestępstwa, których dotyczy postępowanie
 - Inne kraje zaangażowane w sprawę
 - Czy sprawą zajmuje się już Eurojust?
 - Jeżeli tak, identyfikator sprawy Eurojustu?
 - Jeśli nie, czy jest to wniosek o wsparcie?

- Czy sprawą zajmuje się Europol?
 - Jeżeli tak, operacyjna grupa zadaniowa („OTF”) lub aplikacja sieci bezpiecznej wymiany informacji („SIENA”)?
 - Umowa o powołaniu zespołu JIT:
 - Państwa, których dotyczy ten projekt
 - Strony umowy o powołaniu zespołu JIT (organy krajowe odpowiedzialne za dochodzenia)
 - Krajowy numer referencyjny postępowania karnego prowadzonego przez zespół JIT
 - Data złożenia podpisu
 - Czas trwania
 - Przestępstwa, których dotyczy postępowanie
 - Krótkie streszczenie sprawy
 - Główni podejrzani w postępowaniu karnym prowadzonym przez zespół JIT (imię, nazwisko, data i miejsce urodzenia oraz ewentualnie inne istotne i niezbędne kategorie danych zgodnie z załącznikiem II)
 - Wyniki prac zespołów JIT:
 - Trudności/opóźnienia w zakresie:
 - tworzenia zespołu JIT
 - zwrócenia się o dowody/udostępnienia dowodów w ramach zespołu JIT
 - uzgodnienia/wdrożenia wspólnej strategii ścigania
 - Dopuszczalność/niedopuszczalność/ocena dowodów zgromadzonych przez zespół JIT w postępowaniu krajowym
 - Wynik postępowania sądowego (postępowania karne zakończone powodzeniem/niepowodzeniem oraz wyroki skazujące/uniewinniające)
- (iii) Kod uprzedniej zgody
- b) Art. 21 ust. 5 rozporządzenia (UE) 2018/1727, poważne sprawy złożone
- (i) Sekcja najwyższego poziomu
Ta sekcja najwyższego poziomu odpowiada informacjom określonym w art. 21 ust. 5 rozporządzenia w sprawie Eurojustu: poważne sprawy złożone
 - (ii) Struktura wiadomości
Struktura danych składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:
 - Krajowy organ sądowy odpowiedzialny za postępowanie karne
 - Krajowy numer referencyjny postępowania karnego
 - Status postępowania karnego
 - Przestępstwa, których dotyczy postępowanie
 - Inne kraje zaangażowane w sprawę
 - Czy sprawą zajmuje się już Eurojust?
 - Jeżeli tak, identyfikator sprawy Eurojustu?
 - Jeśli nie, czy jest to wniosek o wsparcie?

- Czy sprawą zajmuje się Europol?
 - Jeżeli tak, operacyjna grupa zadaniowa lub SIENA?
 - Właściwa forma poważnej przestępczości
 - Udział zorganizowanej grupy przestępczej
 - Typu mafijnego
 - Międzynarodowa zorganizowana grupa przestępcza
 - Reperkusje na szczeblu UE
 - Główni podejrzani w postępowaniu karnym (imię, nazwisko, data i miejsce urodzenia oraz ewentualnie inne istotne i niezbędne kategorie danych zgodnie z załącznikiem II)
 - Krótkie streszczenie sprawy
 - Inne zaangażowane kraje
 - Kraje, z którymi współpracę już rozpoczęto
 - Właściwe organy zaangażowane w innym państwie
 - Zastosowane instrumenty współpracy wymiarów sprawiedliwości
 - Liczba wysłanych/otrzymanych wniosków
 - Istnienie powiązanych dochodzeń
 - Kraje, z którymi współpraca ma zostać rozpoczęta/kraje potencjalnie dotknięte
 - Typ potrzebnej współpracy (np. ekstradycja, gromadzenie dowodów, inna współpraca)
 - Istnienie powiązanych dochodzeń
- (iii) Kod uprzedniej zgody
- c) Art. 21 ust. 6 lit. a) rozporządzenia (UE) 2018/1727, konflikty jurysdykcji
- (i) Sekcja najwyższego poziomu
Ta sekcja najwyższego poziomu odpowiada informacjom określonym w art. 21 ust. 6 lit. a) rozporządzenia (UE) 2018/1727: konflikty jurysdykcji
- (ii) Struktura wiadomości
Struktura danych składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:
- Krajowy organ sądowy odpowiedzialny za postępowanie karne
 - Krajowy numer referencyjny postępowania karnego
 - Status postępowania karnego (np. postępowanie przygotowawcze, wnoszenie i popieranie oskarżenia, proces)
 - Przestępstwa, których dotyczy postępowanie
 - Inne kraje zaangażowane w sprawę
 - Czy sprawą zajmuje się już Eurojust?
 - Jeżeli tak, identyfikator sprawy Eurojustu?
 - Jeżeli nie, czy jest to wniosek o wsparcie?

- Czy sprawą zajmuje się Europol?
 - Jeżeli tak, operacyjna grupa zadaniowa lub SIENA?
- Inne zaangażowane kraje
 - Właściwe organy krajowe w innym państwie, jeżeli są znane
 - Krajowy numer referencyjny postępowania karnego w innym państwie
 - Etap postępowania w innym państwie, jeżeli jest znany
- Konflikt pozytywny lub negatywny
- Konflikt rzeczywisty lub potencjalny
 - Czynności koordynacyjne już podjęte (np. konsultacje na mocy decyzji ramowej Rady 2009/948/WSiSW ⁽¹⁾)
- Krótkie streszczenie sprawy
- Główni podejrzani (imię, nazwisko, data i miejsce urodzenia oraz ewentualnie inne istotne i niezbędne kategorie danych zgodnie z załącznikiem II)
- (iii) Kod uprzedniej zgody
- d) Art. 21 ust. 6 lit. b), przesyłki niejawnie nadzorowane
 - (i) Sekcja najwyższego poziomu
Ta sekcja najwyższego poziomu odpowiada informacjom określonym w art. 21 ust. 6 lit. b) rozporządzenia (UE) 2018/1727: przesyłki niejawnie nadzorowane
 - (ii) Struktura wiadomości
Struktura danych składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:
 - Krajowy organ sądowy odpowiedzialny za postępowanie karne
 - Krajowy numer referencyjny postępowania karnego
 - Status postępowania karnego (np. postępowanie przygotowawcze, wnoszenie i popieranie oskarżenia, proces)
 - Przestępstwa, których dotyczy postępowanie
 - Inne kraje zaangażowane w sprawę
 - Czy sprawą zajmuje się już Eurojust?
 - Jeżeli tak, identyfikator sprawy Eurojustu?
 - Jeśli nie, czy jest to wniosek o wsparcie?
 - Czy sprawą zajmuje się Europol?
 - Jeżeli tak, operacyjna grupa zadaniowa lub SIENA?
 - Inne zaangażowane kraje
 - Kraj pochodzenia/tranzytu/przeznaczenia
 - Właściwe organy krajowe w innych krajach
 - Istnienie powiązanych dochodzeń w innych krajach

⁽¹⁾ Decyzja ramowa Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym i w sprawie rozstrzygania takich konfliktów (Dz.U. L 328 z 15.12.2009, s. 42, ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

- Rodzaj dostarczonych towarów (np. narkotyki i ich rodzaj/pieniądze/broń/papierosy/inne)
- Status przesyłki niejawnie nadzorowanej (np. planowana, w trakcie realizacji, dostarczona)
- Wynik, jeżeli przesyłkę niejawnie nadzorowaną już dostarczono
- Zastosowany instrument współpracy wymiarów sprawiedliwości
- Główni podejrzani (imię, nazwisko, data i miejsce urodzenia oraz ewentualnie inne istotne i niezbędne kategorie danych zgodnie z załącznikiem II)
- (iii) Kod uprzedniej zgody
- e) Art. 21 ust. 6 lit. c) rozporządzenia (UE) 2018/1727, powtarzające się problemy związane z instrumentami współpracy wymiarów sprawiedliwości
 - (i) Sekcja najwyższego poziomu

Ta sekcja najwyższego poziomu odpowiada informacjom określonym w art. 21 ust. 6 lit. c) rozporządzenia (UE) 2018/1727: powtarzające się problemy związane z instrumentami współpracy wymiarów sprawiedliwości
 - (ii) Struktura wiadomości

Struktura danych składa się z sekwencji elementów i obejmuje co najmniej następujące informacje:

 - Krajowy organ sądowy odpowiedzialny za postępowanie karne
 - Krajowy numer referencyjny postępowania karnego
 - Status postępowania karnego (np. postępowanie przygotowawcze, wnoszenie i popieranie oskarżenia, proces)
 - Przestępstwa, których dotyczy postępowanie
 - Inne kraje zaangażowane w sprawę
 - Czy sprawą zajmuje się już Eurojust?
 - Jeżeli tak, identyfikator sprawy Eurojustu?
 - Jeśli nie, czy jest to wniosek o wsparcie?
 - Czy sprawą zajmuje się Europol?
 - Jeżeli tak, operacyjna grupa zadaniowa lub SIENA?
 - Inne zaangażowane kraje
 - Właściwe organy krajowe, jeżeli są znane
 - Działanie w charakterze organu wydającego lub wykonującego
 - Instrument współpracy wymiarów sprawiedliwości (np. ENA, END, zabezpieczenie i konfiskata)
 - Przedmiot danego wniosku (tj. jaka czynność dochodzeniowa, rodzaj zabezpieczenia, ENA w celu wykonania wyroku czy ścigania)
 - Odmowa lub powtarzające się trudności
 - W przypadku odmowy – na jakiej konkretnej podstawie?
 - Krótki opis problemu
 - Inne organy krajowe dotknięte tym samym problemem, jeżeli istnieją
 - (iii) Kod uprzedniej zgody

2.3. *Kody uprzedniej zgody*

Udostępniając dane Eurojustowi za pośrednictwem systemu JUDEX właściwe organy krajowe wskazują za pomocą kodów uprzedniej zgody dalsze przetwarzanie danych, dostęp do nich i ich przekazywanie po stwierdzeniu powiązania. Kody uprzedniej zgody wskazują, czy i w jakim zakresie informacje odnoszące się do powiązania mogą być udostępniane innym właściwym organom krajowym, innym agencjom i organom Unii, państwom trzecim lub organizacjom międzynarodowym.

2.4. *Uprzednio zdefiniowane wiadomości*

Uprzednio zdefiniowane wiadomości to formy wymiany informacji ustanowionej w rozporządzeniu (UE) 2018/1727, ale w przypadku których w akcie prawnym nie przewidziano żadnego konkretnego formatu. Ich rodzaje i liczbę określa się w trakcie analizy biznesowej i technicznej.

Definicje schematów XLM (XSD) dla uprzednio zdefiniowanych wiadomości projektuje się w taki sposób, aby zapewnić spójność, strukturę i zgodność z potrzebami biznesowymi.

Do tych schematów stosuje się następujące zasady:

- a) sekcja najwyższego poziomu w tym schemacie musi nosić nazwę odpowiadającą konkretnemu rodzajowi definiowanej wiadomości;
- b) w ramach tej struktury dodaje się i określa niezbędne pola wymagane dla konkretnego rodzaju wiadomości, zapewniając właściwe przedstawienie elementów danych.

2.5. *Wiadomości tekstowe*

Wiadomości tekstowe to formy prezentacji wymiany informacji, umożliwiające przekazywanie nieustrukturyzowanych lub częściowo ustrukturyzowanych treści, co pozwala na elastyczność przy jednoczesnym zachowaniu zgodności z wymogami regulacyjnymi i biznesowymi. Schematy XSD dla wiadomości tekstowych projektuje się w taki sposób, aby zapewnić spójność i właściwe formatowanie.

Do tych schematów stosuje się następujące zasady:

- a) sekcja najwyższego poziomu w schemacie musi nosić nazwę odpowiadającą konkretnemu rodzajowi definiowanej wiadomości tekstowej;
- b) w schemacie określa się niezbędną strukturę wiadomości tekstowej, zarazem umożliwiając odpowiednie uporządkowanie elementów w zależności od wymogów;
- c) w ramach tej struktury dodaje się i określa niezbędne pola wymagane dla konkretnego rodzaju wiadomości tekstowej, zapewniając właściwe przedstawienie elementów danych.

ZAŁĄCZNIK III

SPECYFIKACJE TECHNICZNE DOTYCZĄCE ODCISKÓW PALCÓW I FOTOGRAFII

Wiadomościom wymienianym za pośrednictwem zdecentralizowanego systemu teleinformatycznego mogą towarzyszyć załączniki, w tym pliki Narodowego Instytutu Standaryzacji i Technologii („NIST”) zawierające odciski palców i fotografie, zgodnie ze specyfikacjami technicznymi określonymi w pkt 1 i 2.

1. Odciski palców

Odciski palców, które mogą być udostępniane Eurojustowi w celu wiarygodnej identyfikacji osób, wobec których toczy się postępowanie karne dotyczące przestępstw terrorystycznych, spełniają następujące warunki:

- a) odciski palców umieszcza się w jednym pliku zawierającym cyfrowe obrazy odcisków palców (plik NIST z odciskami palców) i przesyła się je zgodnie z normą ANSI/NIST-ITL 1-2011, aktualizacja z 2015 r. (lub nowszą wersją);
- b) plik NIST obejmuje maksymalnie dziesięć pojedynczych odcisków palców: przetoczonych, płaskich bądź obu rodzajów;
- c) wszystkie odciski palców są opisane;
- d) odciski palców pobrano w formie skanu na żywo lub tuszowego odcisku na papierze, przy czym odciski palców sporządzone metodą tuszową na papierze muszą być zeskanowane w wymaganej rozdzielczości i w tej samej jakości;
- e) plik NIST z odciskami palców umożliwia uwzględnienie informacji uzupełniających, takich jak warunki rejestracji odcisków palców oraz metoda stosowana do pozyskania poszczególnych obrazów odcisków palców;
- f) odciski palców mają nominalną rozdzielczość 500 albo 1 000 ppi⁽¹⁾ (z dopuszczalnym odchyleniem ± 10 ppi) w 256 odcieniach szarości;
- g) stosowany algorytm kompresji odcisków palców jest zgodny z zaleceniami Narodowego Instytutu Standaryzacji i Technologii („NIST”). Dane daktyloskopijne o rozdzielczości 500 ppi są kompresowane przy użyciu algorytmu WSQ (ISO/IEC 19794-5:2005). Dane daktyloskopijne o rozdzielczości 1 000 ppi są kompresowane przy użyciu standardu kompresji obrazów JPEG 2000 (ISO/IEC 15444-1) i systemu kodowania. Docelowy współczynnik kompresji wynosi 15:1.

2. Fotografie

Fotografie, które mogą być udostępniane Eurojustowi w celu wiarygodnej identyfikacji osób, wobec których toczy się postępowanie karne dotyczące przestępstw terrorystycznych, spełniają następujące warunki:

- a) plik fotografii (plik fotografii NIST) zawiera tylko jeden wizerunek twarzy i jest przesyłany zgodnie z normą ANSI/NIST-ITL 1-2011, aktualizacja z 2015 r. lub z jej nowszą wersją, o ile jest dostępna;
- b) fotografie są w skali szarości, kolorze lub bliskiej podczerwieni;
- c) jakość fotografii odpowiada wymogom dotyczącym wizerunku w pozycji frontalnej określonym w normie ISO/IEC 19794-5:2011 lub w jej nowszej wersji, o ile jest dostępna;
- d) plik z fotografią NIST umożliwia uwzględnienie informacji uzupełniających, w tym daty wykonania fotografii;

⁽¹⁾ Piksele na cal.

- e) fotografie w trybie portretowym mają minimalną rozdzielczość 600 pikseli na 800 pikseli i maksymalną rozdzielczość 1 200 pikseli na 1 600 pikseli;
 - f) twarz zajmuje w obrębie fotografii taką przestrzeń, aby odległość między środkami oczu wynosiła co najmniej 120 pikseli;
 - g) stosowany algorytm kompresji fotografii jest zgodny z zaleceniami Narodowego Instytutu Standaryzacji i Technologii („NIST”). fotografie poddaje się kompresji tylko raz przy użyciu standardu kompresji obrazu JPG (ISO/IEC 10918) lub JPEG 2000 (ISO/IEC 15444) i systemu kodowania, przy maksymalnym dopuszczalnym współczynniku kompresji obrazu wynoszącym 20:1.
-