KOMISJA
EUROPEJSKA

Bruksela, dnia 25.7.2022 r.
COM(2022) 364 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Pierwsze sprawozdanie dotyczące stosowania i funkcjonowania dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Pierwsze sprawozdanie dotyczące stosowania i funkcjonowania dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych

Spis treści

1 Dyrektywa o ochronie danych w sprawach karnych jako główny instrument zapewniający ochronę danych w ramach polityki bezpieczeństwa Unii Europejskiej 3

1.1 Kluczowy element spójnych unijnych ram ochrony danych 3

1.2 Znaczący wkład w realizację solidnej polityki bezpieczeństwa w Unii Europejskiej 6

1.3 Ważne uwagi dotyczące przygotowania sprawozdania 7

2 Poziom transpozycji jest zadowalający, ale pozostaje szereg nierozwiązanych kwestii 9

2.1 Zasadniczo dokonano pełnej transpozycji, ale z pewnymi niedociągnięciami w zakresie przepisów szczegółowych 10

2.2 Priorytety oceny zgodności 10

2.2.1 Zakres dyrektywy o ochronie danych w sprawach karnych 12

2.2.2 Zarządzanie organami nadzorującymi ochronę danych oraz ich uprawnienia 13

2.2.3 Środki zaradcze 15

2.2.4 Terminy przechowywania i przeglądu 16

2.2.5 Podstawa prawna przetwarzania danych osobowych, w tym ich szczególnych kategorii 16

2.2.6 Zautomatyzowane podejmowanie decyzji 17

2.2.7 Prawa osoby, której dane dotyczą 18

2.2.8 Niektóre ważne przepisy specyficzne dla dyrektywy o ochronie danych w sprawach karnych 18

3 Pierwsze wnioski ze stosowania i funkcjonowania dyrektywy o ochronie danych w sprawach karnych 20

3.1 Skargi oraz pozytywny wpływ na prawa osób, których dane dotyczą 20

3.2 Zwiększona świadomość w zakresie ochrony danych wśród właściwych organów 21

3.3 Bezpieczeństwo danych zwiększyło się, choć występują rozbieżności w zakresie powiadomień o naruszeniu ochrony danych 23

3.4 Nadzór sprawowany przez organy nadzorujące ochronę danych 24

3.4.1 Zasoby organów nadzorujących ochronę danych 24

3.4.2 Korzystanie z uprawnień 26

3.4.3 Kontrola sądowa działania organów nadzorujących ochronę danych 28
3.4.4 Wytyczne EROD 28
3.4.5 Wzajemna pomoc 30
3.5 Elastyczny instrument międzynarodowego przekazywania danych 30
3.5.1 Decyzje stwierdzające odpowiedni stopień ochrony 31
3.5.2 Odpowiednie zabezpieczenia 32
3.5.3 Stosowanie wyjątków 38
3.5.4 Skuteczna współpraca policyjna i sądowa ponad granicami 38
4 Dalsze działania 40

1 DYREKTYWA O OCHRONIE DANYCH W SPRAWACH KARNYCH JAKO GŁÓWNY INSTRUMENT ZAPEWNIAJĄCY OCHRONĘ DANYCH W RAMACH POLITYKI BEZPIECZEŃSTWA UNII EUROPEJSKIEJ

W niniejszym komunikacie przedstawiono pierwsze sprawozdanie Komisji Europejskiej z oceny i przeglądu dyrektywy (UE) 2016/680 o ochronie danych w sprawach karnych („dyrektywa o ochronie danych w sprawach karnych")[1], na podstawie art. 62 ust. 1 tej dyrektywy.

W sprawozdaniu przeanalizowano w szczególności stosowanie i funkcjonowanie przepisów dyrektywy o ochronie danych w sprawach karnych dotyczących przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych, zgodnie z wymogiem tej dyrektywy, ale przyjęto w nim również szersze podejście. Jak wynika z niniejszego sprawozdania, dyrektywa o ochronie danych w sprawach karnych stanowi część prawa UE dotyczącego danych osobowych i prawa UE regulującego przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom („ściganie przestępstw")[2]. Sprawozdanie zawiera przegląd transpozycji dyrektywy o ochronie danych w sprawach karnych do prawa krajowego państw członkowskich, przedstawia pierwsze wnioski wyciągnięte z jej stosowania i funkcjonowania oraz określa dalsze działania.

1.1 Kluczowy element spójnych unijnych ram ochrony danych

Dyrektywa o ochronie danych w sprawach karnych jest jednym z trzech filarów unijnych ram gwarantujących prawo podstawowe do ochrony danych osobowych. Pozostałe dwa to ogólne rozporządzenie o ochronie danych („RODO")[3] i rozporządzenie o ochronie danych przez instytucje i organy Unii[4]. Prawo podstawowe do ochrony danych zapisano w art. 8 Karty praw podstawowych Unii Europejskiej („Karta")[5] i art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE")[6].

---

[1] Dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

[2] Art. 1 ust. 1 dyrektywy o ochronie danych w sprawach karnych.

[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 (Dz.U. L 119 z 4.5.2016, s. 1).

[4] 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).

[5] Karta praw podstawowych Unii Europejskiej (Dz.U. C 202 z 7.6.2016, s. 389).

[6] Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej (Dz.U. C 202 z 7.6.2016, s. 47).

Dyrektywa o ochronie danych w sprawach karnych weszła w życie 6 maja 2016 r., a państwa członkowskie były zobowiązane do jej transpozycji do prawa krajowego do 6 maja 2018 r.[7]

Dyrektywa ta jest pierwszym unijnym aktem ustawodawczym, w którym przyjęto kompleksowe podejście do ochrony danych osobowych przez właściwe organy (tj. organy sądowe, policję i inne organy ścigania, o których mowa w art. 3 pkt 7 dyrektywy) do celów ścigania przestępstw. W porównaniu z decyzją ramową Rady 2008/977/WSiSW[8], którą dyrektywa o ochronie danych w sprawach karnych uchyliła i zastąpiła, dyrektywa ta stanowi istotny postęp w dążeniu do zapewnienia spójnego stosowania przepisów o ochronie danych w całej UE. Po pierwsze, dyrektywa o ochronie danych w sprawach karnych zawiera kompletny zbiór przepisów dotyczących przetwarzania zarówno na szczeblu transgranicznym, jak i krajowym danych osobowych do celów ścigania przestępstw, a decyzja ramowa Rady obejmowała jedynie transgraniczne przetwarzanie. Po drugie, dyrektywa o ochronie danych w sprawach karnych zawiera kompleksowy i horyzontalny zestaw przepisów, podczas gdy zgodnie z poprzednim podejściem każdy unijny akt sektorowy, który dotyczył przetwarzania danych osobowych w kontekście ścigania przestępstw, podlegał osobnym przepisom o ochronie danych[9].

Ogólne rozporządzenie o ochronie danych, rozporządzenie o ochronie danych przez instytucje i organy Unii oraz dyrektywa o ochronie danych w sprawach karnych są oparte na podobnych koncepcjach i zasadach[10], co zapewnia spójną wykładnię i spójne stosowanie unijnych przepisów o ochronie danych. We wszystkich tych aktach prawnych zawarto wspólne definicje i określono podobne obowiązki administratorów danych i podmiotów przetwarzających. Dyrektywa o ochronie danych w sprawach karnych dotyczy jednak także w szczególności ryzyka związanego z przetwarzaniem danych osobowych w kontekście ścigania przestępstw. Odpowiednie przepisy obejmują obowiązki (i) rozróżniania poszczególnych kategorii osób, których dane dotyczą, (ii) rozróżniania pomiędzy danymi osobowymi opartymi na faktach a danymi osobowymi opartymi na indywidualnych ocenach, (iii) prowadzenia ewidencji wykorzystania danych osobowych i spełnienia określonych wymogów bezpieczeństwa[11].

Biorąc pod uwagę szczególny charakter współpracy sądowej w sprawach karnych i współpracy policyjnej, uznano za konieczne przyjęcie w tych dziedzinach szczegółowych przepisów dotyczących ochrony danych osobowych i swobodnego przepływu danych osobowych[12].

---

[7] Art. 63 ust. 1 dyrektywy o ochronie danych w sprawach karnych.

[8] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.U. L 350 z 30.12.2008, s. 60).

[9] Na przykład akty prawne regulujące System Informacyjny Schengen i inne instrumenty stanowiące dorobek Schengen zawierały przepisy szczegółowe regulujące takie kwestie, jak prawa osób, których dane dotyczą.

[10] Należą do nich zgodność z prawem i rzetelność; ograniczenie celu; minimalizacja danych; prawidłowość; ograniczenie przechowywania; integralność i poufność oraz rozliczalność (art. 4 dyrektywy o ochronie danych w sprawach karnych).

[11] Odpowiednio art. 6, 7, 25 i 29 dyrektywy o ochronie danych w sprawach karnych.

[12] Deklaracja nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączona do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony (Dz.U. C 115 z 9.5.2008, s. 345).

Wrażliwy charakter obszaru, jakim jest współpraca wymiarów sprawiedliwości w sprawach karnych i współpraca policyjna, jak również złożoność krajowych ram prawnych regulujących ściganie przestępstw, przyczyniły się do uznania dyrektywy za najlepszy instrument osiągnięcia wysokiego poziomu ochrony danych w tej dziedzinie. Dyrektywa pozostawia również państwom członkowskim niezbędną elastyczność we wdrażaniu tych zasad, przepisów i wyjątków na szczeblu krajowym[13].

Komisja opublikowała swoje pierwsze sprawozdanie z wdrażania RODO 24 czerwca 2020 r.[14] Stwierdzono w nim ogólnie, że RODO spełnia swoje cele, w szczególności zapewniając obywatelom solidny zestaw egzekwowalnych praw oraz tworząc nowy unijny system zarządzania i egzekwowania. W sprawozdaniu określono działania, które należy podjąć w celu dalszego ułatwiania stosowania RODO przez wszystkie zainteresowane strony, a także promowania i dalszego rozwoju kultury ochrony danych w UE oraz stanowczego egzekwowania przepisów.

Niniejsze sprawozdanie stanowi kontynuację przeglądu przyjętych przez UE aktów prawnych regulujących przetwarzanie danych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar. Celem tego przeglądu była ocena potrzeby dostosowania wspomnianych aktów prawnych do dyrektywy o ochronie danych w sprawach karnych[15]. 24 czerwca 2020 r. Komisja wypełniła ten obowiązek, przyjmując komunikat „Dalsze działania dotyczące dostosowania dotychczasowego dorobku w obszarze trzeciego filaru do przepisów o ochronie danych”[16]. W ramach przeglądu zidentyfikowano 10 aktów prawnych, które należy dostosować do dyrektywy o ochronie danych w sprawach karnych, a także ustalono harmonogram tych działań.

Ponadto niniejsze sprawozdanie zostało przygotowane równolegle ze sprawozdaniem Komisji dotyczącym stosowania rozporządzenia o ochronie danych przez instytucje i organy Unii. Ważnym elementem tego ostatniego sprawozdania jest przegląd przepisów rozdziału IX tego rozporządzenia, dotyczących przetwarzania operacyjnych danych osobowych przez organy lub jednostki organizacyjne UE podczas prowadzenia działań wchodzących w zakres współpracy

[13] Uzasadnienie wniosku dotyczącego dyrektywy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM(2012) 10 final, 25 stycznia 2012 r.

[14] Komunikat Komisji do Parlamentu Europejskiego i Rady „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych”, COM(2020) 264 final, 24 czerwca 2020 r.

[15] Art. 62 ust. 6 dyrektywy o ochronie danych w sprawach karnych nałożył na Komisję obowiązek dokonania do 6 maja 2019 r. przeglądu innych aktów prawnych UE regulujących przetwarzanie danych osobowych do celów ścigania przestępstw w celu oceny, czy konieczne jest dostosowanie ich do tej dyrektywy, i w razie potrzeby przedstawienia propozycji zmiany takich aktów prawnych UE dla zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres stosowania dyrektywy.

[16] Komunikat Komisji do Parlamentu Europejskiego i Rady „Dalsze działania dotyczące dostosowania dotychczasowego dorobku w obszarze trzeciego filaru do przepisów o ochronie danych”, COM(2020) 262 final, 24 czerwca 2020 r.

policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych[17] („agencje WSiSW”). Wspomniane przepisy opierają się w dużej mierze na dyrektywie o ochronie danych w sprawach karnych. Art. 98 rozporządzenia o ochronie danych przez instytucje i organy Unii zobowiązuje Komisję do dokonania przeglądu aktów prawnych, które regulują przetwarzanie operacyjnych danych osobowych przez agencje WSiSW, i umożliwia jej składanie odpowiednich wniosków ustawodawczych, w szczególności w celu stosowania przepisów rozdziału IX do Europolu[18] i Prokuratury Europejskiej, a także proponowanie wszelkich niezbędnych zmian w tym rozdziale.

1.2 Znaczący wkład w realizację solidnej polityki bezpieczeństwa w Unii Europejskiej

Komisja niezmiennie podkreśla, że tylko pełne przestrzeganie praw podstawowych zapisanych w Karcie i w prawie wtórnym UE pozwoli budować skuteczną i prawdziwie bezpieczną Unię. Dyrektywa o ochronie danych w sprawach karnych ma kluczowe znaczenie dla polityki bezpieczeństwa UE, ponieważ zapewnia należytą ochronę danych osobowych ofiar, świadków i podejrzanych o popełnienie przestępstwa. Ponadto dzięki harmonizacji przepisów dotyczących ochrony danych osobowych przetwarzanych przez właściwe organy w państwach UE i państwach obszaru Schengen dyrektywa ta przyczynia się do zwiększenia zaufania i bezpieczeństwa wymiany danych między organami na potrzeby ścigania przestępstw, a tym samym ułatwia współpracę transgraniczną w zakresie zwalczania przestępczości i terroryzmu[19]. Dyrektywa o ochronie danych w sprawach karnych odgrywa również kluczową rolę w promowaniu kultury przestrzegania ochrony danych przez właściwe organy.

W strategii w zakresie unii bezpieczeństwa[20] podkreślono ponadto, że nowe technologie, takie jak sztuczna inteligencja, mogą znaleźć zastosowanie jako potężne narzędzie do zwalczania przestępczości. Wykorzystanie tego potencjału oznacza również zapewnienie najwyższych standardów przestrzegania praw podstawowych. Prawodawstwo w zakresie ochrony danych, w tym dyrektywa o ochronie danych w sprawach karnych, stanowi podstawę do konstruowania przepisów sektorowych. Na przykład w proponowanym akcie w sprawie sztucznej inteligencji[21] zostaną ustanowione szczegółowe przepisy dotyczące wykorzystania danych osobowych na potrzeby zdalnej identyfikacji biometrycznej w miejscach publicznych do celów ścigania przestępstw.

Co więcej, w świecie pełnym wzajemnych powiązań przestępczość (w szczególności cyberprzestępczość oraz inne formy przestępczości wykorzystującej cyberprzestrzeń) coraz

[17] Część trzecia tytuł V rozdziały 4 i 5 TFUE.
[18] Tę kwestię omówiono już we wniosku Komisji z 2020 r. dotyczącym zmiany rozporządzenia w sprawie Europolu.
[19] Komunikat Komisji do Parlamentu Europejskiego i Rady – Pierwsze sprawozdanie z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa, COM(2020) 797 final, 9 grudnia 2020 r.
[20] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa, COM(2020) 605 final, 24 lipca 2020 r.
[21] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii, COM(2021) 206 final, 21 kwietnia 2021 r.

częściej ma charakter transgraniczny. Nawet podczas prowadzenia postępowań przygotowawczych w sprawach krajowych właściwe organy w coraz większym stopniu spotykają się sytuacjami o charakterze transgranicznym, ponieważ informacje są przechowywane w formie elektronicznej w kraju trzecim. W tym kontekście zwiększa się potrzeba współpracy międzynarodowej w zakresie postępowań przygotowawczych w sprawach karnych, zarówno ze strony organów państw członkowskich, jak i ze strony organów UE, takich jak Europol czy Eurojust. Tego rodzaju współpraca, w szczególności zbieranie i wymiana elektronicznych materiałów dowodowych,[22] często wiąże się z przekazywaniem danych osobowych. Niezbędne są zatem silne zabezpieczenia dotyczące ochrony danych. Zabezpieczenia tego rodzaju umożliwiają również budowanie zaufania między organami ścigania, zapewniając przy tym szybszą i bardziej skuteczną wymianę informacji oraz przyczyniając się do poprawy pewności prawa, jeżeli informacje są następnie wykorzystywane w postępowaniach karnych. W tym względzie w dyrektywie o ochronie danych w sprawach karnych przewidziano zaktualizowany zestaw narzędzi ułatwiających przekazywanie danych osobowych z UE do państwa trzeciego lub organizacji międzynarodowej (np. Interpolu[23]), przy jednoczesnym zapewnieniu dalszego korzystania z wysokiego poziomu ochrony danych osobowych. Od momentu wejścia w życie dyrektywy o ochronie danych w sprawach karnych Komisja i państwa członkowskie wykorzystały całą gamę przewidzianych w niej narzędzi, potwierdzając w ten sposób, że zastosowane w niej podejście jest wystarczająco wszechstronne i elastyczne, aby umożliwić skuteczną współpracę policyjną i sądową na szczeblu międzynarodowym.

1.3 Ważne uwagi dotyczące przygotowania sprawozdania

Przygotowując niniejsze sprawozdanie, Komisja zebrała informacje zwrotne i opinie z różnych źródeł oraz poprzez ukierunkowane działania konsultacyjne. Zgodnie z art. 62 dyrektywy o ochronie danych w sprawach karnych Komisja uwzględniła stanowiska i ustalenia Parlamentu

[22] W około 85 % postępowań przygotowawczych w sprawie poważnych przestępstw potrzebne są informacje i dowody elektroniczne, a 65 % wszystkich wniosków o ich udostępnienie kieruje się do dostawców usług mających siedzibę w innym kraju. Zob. dokument roboczy służb Komisji („Ocena skutków towarzysząca wnioskowi w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych oraz wniosek w sprawie dyrektywy Parlamentu Europejskiego i Rady ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych”), SWD(2018) 118 final.

[23] Zob. również motyw 25 dyrektywy o ochronie danych w sprawach karnych.

Europejskiego[24], Rady[25], Europejskiej Rady Ochrony Danych (EROD)[26] oraz krajowych organów nadzorujących ochronę danych. Dodatkowe informacje zwrotne uzyskano dzięki kwestionariuszowi skierowanemu do organizacji społeczeństwa obywatelskiego (za pośrednictwem Agencji Praw Podstawowych Unii Europejskiej)[27] oraz odpowiedziom na publiczne zaproszenie do zgłaszania uwag[28]. Komisja uwzględniła także uwagi grupy ekspertów z państw członkowskich ds. RODO i dyrektywy o ochronie danych w sprawach karnych[29] oraz uwagi niemieckiej prezydencji w Radzie Unii Europejskiej[30]. Wzięła również pod uwagę analizę krajowych środków transpozycji oraz niewielką liczbę skarg, które w tym względzie otrzymała.

Chociaż dyrektywa o ochronie danych w sprawach karnych ma zastosowanie do wszystkich państw członkowskich oraz wszystkich krajów należących do strefy Schengen (ponieważ stanowi rozwinięcie dorobku prawnego Schengen[31]), niniejsze sprawozdanie obejmuje wyłącznie państwa członkowskie UE.

Na przygotowanie niniejszego sprawozdania miały wpływ trzy czynniki. Po pierwsze, dwie trzecie państw członkowskich nie wywiązało się z wyznaczonego na maj 2018 r. terminu transpozycji dyrektywy o ochronie danych w sprawach karnych do prawa krajowego. Większość państw członkowskich dokonała jednak transpozycji dyrektywy o ochronie danych w sprawach karnych w 2019 r., po wszczęciu przez Komisję postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego. Doświadczenie w zakresie jej stosowania jest raczej ograniczone, co podkreślają również EROD[32] i Rada[33]. Po drugie, opracowanie statystyk dotyczących stosowania

---

[24] Wkład Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego do przygotowywanego obecnie przez Komisję Europejską sprawozdania z oceny i przeglądu dyrektywy o ochronie danych w sprawach karnych, 7 lutego 2022 r.

[25] Stanowisko i ustalenia Rady dotyczące stosowania dyrektywy o ochronie danych w sprawach karnych (dokument Rady 13943/21 z 18 listopada 2021 r. https://www.consilium.europa.eu/media/54304/st_13943_2021_init_en.pdf).

[26] Wkład EROD w sporządzoną przez Komisję Europejską ocenę dyrektywy o ochronie danych w sprawach karnych na podstawie art. 62 tej dyrektywy, dokument przyjęty 14 grudnia 2021 r. („wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych").
https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

[27] Spośród 804 organizacji społeczeństwa obywatelskiego, do których zwróciła się Agencja Praw Podstawowych Unii Europejskiej (FRA), odpowiedzi udzieliło 88. Możliwe było jednak uwzględnienie tylko 17 z tych *odpowiedzi ze względu na to, że 61 odpowiedzi nie miało związku z dyrektywą o ochronie danych w sprawach karnych* lub wskazywało, że dana organizacja nie pracuje nad ochroną praw podstawowych w dziedzinie ścigania przestępstw lub w ogóle nie zna dyrektywy o ochronie danych w sprawach karnych.

[28] Zaproszenie do zgłaszania uwag, ochrona danych w ściganiu przestępstw – sprawozdanie dotyczące dyrektywy o ochronie danych w sprawach karnych, 24 stycznia 2022 r. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13288-Ochrona-danych-w-sciganiu-przestepstw-sprawozdanie-dotyczace-dyrektywy-o-ochronie-danych-w-sprawach-karnych_pl.

[29] Grupa ekspertów Komisji ds. rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680 (E03461); https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461

[30] Sprawozdanie prezydencji Rady Unii Europejskiej w sprawie wymiany danych policyjnych z państwami trzecimi – doświadczenia w stosowaniu art. 37 dyrektywy o ochronie danych w sprawach karnych, grudzień 2020 r.

[31] Zob. motywy 101–103 dyrektywy o ochronie danych w sprawach karnych.

[32] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 4.

[33] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 7.

dyrektywy o ochronie danych w sprawach karnych okazało się trudniejsze niż w przypadku RODO. Niektóre organy nadzorujące ochronę danych nie gromadzą danych statystycznych dotyczących prowadzonych działań nadzorczych odrębnie w odniesieniu do dyrektywy o ochronie danych w sprawach karnych i w odniesieniu do RODO. Dzieje się tak na przykład w odniesieniu do zgłoszeń naruszenia ochrony danych[34] oraz skarg składanych na podstawie dyrektywy o ochronie danych w sprawach karnych[35], co w niektórych przypadkach utrudnia przeprowadzenie dokładnego przeglądu tych przepisów wynikających z dyrektywy o ochronie danych w sprawach karnych[36].

Po trzecie, należy zwrócić uwagę na to, że orzecznictwo dotyczące stosowania dyrektywy o ochronie danych w sprawach karnych dopiero zaczyna być rozwijane. Przed Trybunałem Sprawiedliwości Unii Europejskiej („TSUE") toczy się obecnie kilka postępowań dotyczących interpretacji kluczowych zapisów dyrektywy o ochronie danych w sprawach karnych, takich jak prawo dostępu osób, których dane dotyczą, oraz prawo do skutecznego środka prawnego przed sądem. Wyroki w tych postępowaniach zapewnią większą jasność oraz przyczynią się do stworzenia bardziej zharmonizowanego podejścia wśród państw członkowskich.

2 POZIOM TRANSPOZYCJI JEST ZADOWALAJĄCY, ALE POZOSTAJE SZEREG NIEROZWIĄZANYCH KWESTII

Komisja powołała grupę ekspertów z państw członkowskich,[37] aby pomóc państwom członkowskim włączyć przepisy dyrektywy o ochronie danych w sprawach karnych do ich prawa krajowego. Grupa wspomaga prowadzenie dyskusji oraz wymianę doświadczeń między państwami członkowskimi oraz Komisją na temat przepisów o ochronie danych. Posiedzenia grupy odbywały się regularnie w okresie między przyjęciem dyrektywy o ochronie danych w sprawach karnych w 2016 r. a terminem jej transpozycji wyznaczonym na maj 2018 r., a następnie grupa wznowiła swoje prace w 2021 r.

Przedstawiony poniżej przegląd transpozycji dotyczy przede wszystkim najważniejszych zidentyfikowanych do tej pory kwestii. Podstawę przeglądu stanowi przede wszystkim wykonana przez Komisję analiza informacji, które przekazały jej państwa członkowskie, powiadamiając Komisję o środkach krajowych wprowadzonych w celu transpozycji dyrektywy o ochronie danych w sprawach karnych do prawa krajowego. Analizę tę uzupełniono o badanie zewnętrzne przeprowadzone przez wykonawcę zewnętrznego. Komisja zorganizowała również dwustronne wymiany uwag z kilkoma państwami członkowskimi.

---

[34] Przykładowo organy w Danii, na Litwie, w Norwegii, Austrii i niektóre organy w Niemczech nie prowadzą osobnych statystyk dotyczących naruszeń ochrony danych w ramach dyrektywy o ochronie danych w sprawach karnych. Sześć organów zgłosiło także, że nie otrzymało żadnych zgłoszeń o naruszeniach na podstawie dyrektywy o ochronie danych w sprawach karnych.

[35] Przykładowo organy w Danii i Austrii oraz niektóre organy w Niemczech nie prowadzą odrębnych statystyk dotyczących skarg składanych na podstawie dyrektywy o ochronie danych w sprawach karnych.

[36] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 43.

[37] Zob. przypis 29.

2.1 Zasadniczo dokonano pełnej transpozycji, ale z pewnymi niedociągnięciami w zakresie przepisów szczegółowych

W lipcu 2018 r. Komisja wszczęła postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko 19 państwom członkowskim, które nie wywiązały się z obowiązku przyjęcia przepisów transponujących dyrektywę o ochronie danych w sprawach karnych przed upływem terminu wyznaczonego na maj 2018 r. oraz należytego powiadomienia Komisji o jej transpozycji. W lipcu 2019 r. wszczęte zostało kolejne postępowanie wobec innego państwa członkowskiego w sprawie częściowego braku transpozycji. W konsekwencji większość państw członkowskich powiadomiła następnie Komisję o ustawodawstwie krajowym dokonujących transpozycji, a Komisja stopniowo zamykała prowadzone wobec nich postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego na przestrzeni 2019 r. (w przypadku jednego państwa członkowskiego – w 2020 r.). W 2021 r. Komisja wszczęła przed TSUE postępowanie o naruszenie przeciwko Hiszpanii, ponieważ na tamta chwilę kraj ten nadal nie dokonał transpozycji dyrektywy o ochronie danych w sprawach karnych i nie powiadomił Komisji o przyjętych krajowych środkach transpozycji. Ze względu na wagę i czas trwania naruszenia TSUE po raz pierwszy nałożył na Hiszpanię zarówno karę ryczałtową, jak i okresową karę pieniężną[38].

W kwietniu 2022 r. Komisja wszczęła również postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko Niemcom po wykryciu luki w transpozycji dyrektywy o ochronie danych w sprawach karnych w związku z działaniami niemieckiej policji federalnej.

Komisja będzie nadal oceniać transpozycję dyrektywy o ochronie danych w sprawach karnych przez państwa członkowskie i podejmie działania niezbędne do usunięcia wszystkich braków.

2.2 Priorytety oceny zgodności

Komisja sprawdza również, czy prawidłowo transponowano wymogi dyrektywy o ochronie danych w sprawach karnych do przepisów krajowych państw członkowskich (kontrola zgodności).

Dokonując transpozycji dyrektywy o ochronie danych w sprawach karnych, państwa członkowskie zmieniły wcześniejsze ustawodawstwo dotyczące ochrony danych bądź uchyliły je i zastąpiły nowymi aktami przekrojowymi dotyczącymi ochrony danych. W wielu przypadkach dyrektywa o ochronie danych w sprawach karnych jest transponowana do prawa krajowego poprzez odniesienie do tego samego lub równoważnego przepisu RODO (np. w odniesieniu do definicji, zgłaszania naruszeń ochrony danych, wyznaczania inspektora ochrony danych oraz przepisów dotyczących organizacji, statusu, kompetencji, zadań i uprawnień organów nadzorujących ochronę danych). Transpozycji szeregu przepisów dyrektywy o ochronie danych w sprawach karnych dokonano także poprzez wprowadzenie nowych przepisów, na przykład w zakresie ogólnego prawa administracyjnego, prawa administracyjnego procesowego oraz prawa

[38] Wyrok z 25 lutego 2021 r., Komisja Europejska/Królestwo Hiszpanii, C-658/19, EU:C:2017:548.

karnego procesowego. Niektóre państwa członkowskie dokonały również transpozycji szeregu przepisów dyrektywy o ochronie danych w sprawach karnych poprzez włączenie ich do ustawodawstwa sektorowego regulującego działanie i uprawnienia określonych właściwych organów. Ustalenie, czy dyrektywa o ochronie danych w sprawach karnych została prawidłowo transponowana przez dane państwo członkowskie, może zatem wymagać przeanalizowania szeregu krajowych aktów prawnych. Zasadniczo przepisy prawa krajowego w dużej mierze odzwierciedlają założenia i najważniejsze przepisy dyrektywy o ochronie danych w sprawach karnych. Zidentyfikowano jednak szereg problemów, z których najważniejsze przedstawiono w kolejnych punktach. Komisja wszczęła już szereg postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko państwom członkowskim[39]. Proces przeglądu jest w toku, a Komisja zamierza nadal korzystać ze wszystkich dostępnych narzędzi, w tym postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego, jeżeli krajowy środek transpozycji nie jest zgodny z dyrektywą o ochronie danych w sprawach karnych.

Orzecznictwo dotyczące dyrektywy o ochronie danych osobowych w sprawach karnych jest jeszcze na bardzo wczesnym etapie. TSUE wydał już pierwsze wyroki w sprawie interpretacji dyrektywy o ochronie danych w sprawach karnych, w tym w sprawach WS/Bundesrepublik Deutschland[40] i B/Latvijas Republikas Saeima[41]. W momencie opracowywania niniejszego sprawozdania przed TSUE toczy się szereg postępowań prejudycjalnych (jak wskazano w poniższych sekcjach).

---

[39] W kwietniu 2022 r. Komisja wszczęła postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko Grecji, Finlandii i Szwecji, uzasadniając to tym, że ich przepisy krajowe transponujące dyrektywę nie są zgodne z dyrektywą o ochronie danych w sprawach karnych. Sprawa przeciwko Grecji dotyczy *szeregu kwestii, w tym między innymi* niestosowania prawa krajowego transponującego dyrektywę o ochronie danych w sprawach karnych do przetwarzania danych osobowych przez organy sądowe i organy ścigania oraz inne organy pozostające pod ich nadzorem w przypadku większości czynów zabronionych; transpozycji przepisów dotyczących przechowywania i przeglądu danych (art. 5); podstawy prawnej przetwarzania danych (art. 8) oraz zabezpieczeń w kontekście zautomatyzowanego podejmowania decyzji (art. 11). Przeciwko Finlandii i Szwecji wszczęto postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, ponieważ ich przepisy krajowe nie zapewniają osobom, których dane dotyczą, dostępu do skutecznego środka prawnego przed sądem lub trybunałem. W maju 2022 r. Komisja wszczęła postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego przeciwko Niemcom, ponieważ szereg przepisów krajowych transponujących dyrektywę o ochronie danych w sprawach karnych nie zapewnia skutecznych uprawnień naprawczych na szczeblu federalnym i krajów związkowych.

[40] Wyrok z 12 maja 2021 r., WS/Bundesrepublik Deutschland, C-505/19, EU:C:2021:376. Sprawa, o której mowa, dotyczyła m.in. zgodności z prawem przetwarzania danych osobowych (art. 4 ust. 1 lit. a) i art. 8 dyrektywy o ochronie danych w sprawach karnych) w szczególnym kontekście wydania czerwonej noty Interpolu. Trybunał nie wykluczył przetwarzania danych osobowych zawartych w czerwonej nocie Interpolu jako zgodnego z prawem do czasu ustalenia prawomocnym orzeczeniem sądowym, że do czynów, na których opiera się dana nota, ma zastosowanie zasada *ne bis in idem*.

[41] Wyrok z 22 czerwca 2021 r. B/Latvijas Republikas Saeima, C-439/19, EU:C:2021:504. TSUE dokonał interpretacji definicji właściwego organu zawartej w art. 3 ust. 7 oraz pojęcia przestępczości. Zob. również sekcja poniżej.

2.2.1 Zakres dyrektywy o ochronie danych w sprawach karnych

Zarówno grupa ekspertów z państw członkowskich ds. RODO i dyrektywy o ochronie danych w sprawach karnych[42], jak i EROD[43] zwróciły uwagę na trudność w rozgraniczeniu zakresu stosowania dyrektywy o ochronie danych w sprawach karnych oraz RODO. Niektóre organy nadzorujące ochronę danych również zauważyły, że może to stanowić trudność dla właściwych organów[44].

Zakres dyrektywy o ochronie danych w sprawach karnych jest zdefiniowany[45] przez dwa kluczowe elementy: pojęcie właściwego organu (zakres podmiotowy) i pojęcie czynu zabronionego (zakres przedmiotowy).

Jeżeli chodzi o zakres podmiotowy, przetwarzanie danych wchodzi w zakres dyrektywy o ochronie danych w sprawach karnych, jeżeli, po pierwsze, zajmuje się nim właściwy organ, a po drugie, gdy dane osobowe przetwarza się w celach zgodnych z tą dyrektywą[46] (np. zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom). Zdaniem Komisji „właściwe organy", w rozumieniu dyrektywy o ochronie danych w sprawach karnych[47], to organy państwa lub podmioty prywatne, którym prawo nadaje szczególne uprawnienia wykraczające poza uprawnienia wynikające ze zwykłych przepisów obowiązujących w stosunkach z innymi osobami fizycznymi lub z możliwości stosowania przymusu. Organy te są właściwymi organami zgodnie z dyrektywą o ochronie danych w sprawach karnych, jeżeli (nawet jeżeli wyłącznie sporadycznie lub w odosobnionych przypadkach) przetwarzają dane w celu zapobiegania przestępstwom, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar (w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom). Oznacza to na przykład, że przetwarzanie danych osobowych przez takie organy do celów innych niż dyrektywa o ochronie danych w sprawach karnych (np. do celów związanych z zasobami kadrowymi lub innych celów administracyjnych, takich jak przetwarzanie danych osobowych przez jednostki analityki finansowej (FIU) w ramach dorobku prawnego UE w zakresie przeciwdziałania praniu pieniędzy[48]) jest objęte zakresem stosowania RODO, a nie dyrektywy o ochronie danych w sprawach karnych.

---

[42] Zob. protokół z posiedzenia grupy ekspertów Komisji ds. rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680 z dnia 5 maja 2021 r. https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=pl&meetingId=25283&fromExpertGroups=true

[43] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 7.

[44] Organy nadzorujące ochronę danych z Irlandii, Francji i Węgier wskazały to jako problem.

[45] Art. 2 ust. 1 oraz motywy 12–14 dyrektywy o ochronie danych w sprawach karnych.

[46] Art. 1 dyrektywa o ochronie danych w sprawach karnych.

[47] Art. 3 ust. 7 dyrektywy o ochronie danych w sprawach karnych.

[48] Art. 41 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu

Pojęcie „czyn zabroniony” ma zasadnicze znaczenie przy ustalaniu, czy przetwarzanie danych wchodzi w zakres stosowania dyrektywy o ochronie danych w sprawach karnych. Według TSUE na potrzeby oceny, czy czyn ma charakter zabroniony, istotne są trzy kryteria: to, czy czyn uznaje się za zabroniony na podstawie prawa krajowego, swoisty charakter czynu oraz stopień surowości kary, jaką może ponieść dana osoba[49]. Autonomiczny charakter pojęcia czynu zabronionego, o którym mowa w motywie 13 dyrektywy o ochronie danych w sprawach karnych, oznacza między innymi, że prawo państwa członkowskiego nie może określać charakteru czynu jako „zabronionego” wyłącznie w celu zastosowania dyrektywy o ochronie danych w sprawach karnych.

W niektórych państwach członkowskich pojawia się wątpliwość co do rozgraniczenia zakresu stosowania RODO i dyrektywy o ochronie danych w sprawach karnych w odniesieniu do rozróżnienia między czynami o charakterze karnym i administracyjnym. W szczególności niektóre przepisy krajowe transponujące dyrektywę odnoszą się do celów przetwarzania danych osobowych, których nie wymieniono w art. 1 dyrektywy o ochronie danych w sprawach karnych (np. zagrożeń dla porządku lub bezpieczeństwa publicznego). Wątpliwość ta pojawia się również dlatego, że niektóre państwa członkowskie uważają, że szereg organów administracyjnych (np. wspomniane powyżej jednostki analityki finansowej) wykonuje zadania wchodzące w zakres dyrektywy o ochronie danych w sprawach karnych.

Przepisy większości państw członkowskich w wyczerpujący sposób obejmują wszelkie formy przetwarzania danych przez właściwe organy do celów dyrektywy o ochronie danych w sprawach karnych. Niektóre państwa członkowskie zdecydowały się natomiast na wyczerpujące wyliczenie w swoim ustawodawstwie krajowym właściwych organów działających w ramach dyrektywy o ochronie danych w sprawach karnych. Kilka państw członkowskich przewidziało również odstępstwo dotyczące przetwarzania przez niektóre rodzaje właściwych organów lub przetwarzania niektórych rodzajów danych.

Kwestia zakresu dyrektywy o ochronie danych osobowych w sprawach karnych jest przedmiotem odesłania prejudycjalnego toczącego się przed TSUE. Landesverwaltungsgericht Tirol (sąd w Austrii) poruszył kwestię zakresu stosowania dyrektywy o ochronie danych osobowych w sprawach karnych w sytuacji, gdy właściwy organ bezskutecznie próbował uzyskać dostęp do danych znajdujących się na skonfiskowanym telefonie (wykładnia art. 2 dyrektywy o ochronie danych w sprawach karnych). Sprawa ta dotyczy również warunków takiego dostępu[50].

2.2.2 Zarządzanie organami nadzorującymi ochronę danych oraz ich uprawnienia

Wszystkie państwa członkowskie z wyjątkiem dwóch (Belgia i Szwecja) powierzyły egzekwowanie przepisów dyrektywy o ochronie danych w sprawach karnych organowi

Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE, który reguluje działanie jednostek analityki finansowej, wyraźnie stanowi, że przetwarzanie danych osobowych na podstawie tej dyrektywy podlega rozporządzeniu (UE) 2016/679.

[49] Wyrok z 22 czerwca 2021 r. B/Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, pkt 87.

[50] Wniosek o wydanie orzeczenia w trybie prejudycjalnym w sprawie C.G./Bezirkshauptmannschaft Landeck, C-548/21.

nadzorczemu odpowiedzialnemu również za egzekwowanie RODO. Belgia powierzyła nadzór nad policją do celów dyrektywy o ochronie danych w sprawach karnych innemu organowi nadzorczemu. W Szwecji nadzór nad niektórymi właściwymi organami, w tym policją, sprawują wspólnie organ nadzorczy właściwy ds. RODO oraz inny organ nadzorczy. Co więcej, zgodnie z dyrektywą o ochronie danych w sprawach karnych żaden organ nadzorujący ochronę danych nie jest właściwy do nadzorowania sądów w ramach sprawowania przez nie wymiaru sprawiedliwości.

Jeśli chodzi o przepisy dyrektywy o ochronie danych w sprawach karnych dotyczące niezależności organów nadzorujących ochronę danych[51], wszystkie państwa członkowskie przewidziały w swoich przepisach transponujących, że podczas wykonywania swoich zadań organy nadzorujące ochronę danych działają w sposób niezależny, a członkowie tych organów muszą być wolni od wszelkich wpływów zewnętrznych i nie przyjmować od nikogo poleceń.

Nadzór nad zgodnością z przepisami wykonywany przez organy nadzorujące ochronę danych ma kluczowe znaczenie i został zagwarantowany w art. 8 ust. 3 Karty praw podstawowych. W dyrektywie o ochronie danych w sprawach karnych nakłada się na państwa członkowskie obowiązek zapewnienia, by każdy organ nadzorujący ochronę danych posiadał skuteczne uprawnienia w zakresie prowadzenia postępowań, uprawnienia naprawcze oraz uprawnienia doradcze. To warunek wstępny właściwego egzekwowania przepisów o ochronie danych, a tym samym osiągnięcia celu dyrektywy o ochronie danych w sprawach karnych, jakim jest wysoki stopień ochrony praw podstawowych, w szczególności prawa do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych w UE. Organy nadzorujące ochronę danych muszą posiadać równoważne uprawnienia w całej UE, aby móc wykonywać swoje zadania w sposób określony w dyrektywie o ochronie danych w sprawach karnych[52].

Wszystkie państwa członkowskie przyznały swoim organom uprawnienia w zakresie prowadzenia postępowań określone w dyrektywie o ochronie danych w sprawach karnych, a większość państw członkowskich nadała im również inne uprawnienia (np. do prowadzenia audytów, uzyskiwania dostępu do pomieszczeń, wykonywania kopii danych oraz konfiskowania przedmiotów[53]). W konsekwencji niemal wszystkie organy nadzorujące ochronę danych twierdzą, że posiadają skuteczne uprawnienia w zakresie prowadzenia postępowań.

Niemal wszystkie państwa członkowskie przewidziały uprawnienia naprawcze określone w dyrektywie o ochronie danych w sprawach karnych[54]. Wiele z nich uczyniło to, kierując się

[51] Rozdział VI sekcja 1 dyrektywy o ochronie danych w sprawach karnych.
[52] Motywy 7 i 82 dyrektywy o ochronie danych w sprawach karnych.
[53] Zob. również pkt 23 wkładu EROD w ocenę dyrektywy o ochronie danych w sprawach karnych: 24 państwa członkowskie przewidziały uprawnienia do uzyskiwania dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, a także do sprzętu i środków służących do przetwarzania danych; 21 państw członkowskich przewidziało proces audytu, a 9 państw członkowskich przewidziało inne uprawnienia (np. konfiskowanie przedmiotów, wnioskowanie o przesłuchanie przed organem nadzorującym ochronę danych oraz o pomoc wykonawczą ze strony policji).
[54] Art. 47 ust. 2 lit. a)–c) dyrektywy o ochronie danych w sprawach karnych.

ściśle sformułowaniami zawartymi w dyrektywie o ochronie danych w sprawach karnych, natomiast kilka z nich użyło bardzo szerokich sformułowań, które można racjonalnie interpretować jako obejmujące wszystkie uprawnienia określone w dyrektywie o ochronie danych w sprawach karnych.

Większość państw członkowskich nadała ponadto organom nadzorującym ochronę danych uprawnienia do nakładania administracyjnych kar pieniężnych[55].

Nie wszystkie państwa członkowskie nadały swoim organom nadzorującym ochronę danych uprawnienie do wniesienia do organów sądowych sprawy dotyczącej naruszenia przepisów krajowych przyjętych w celu transpozycji dyrektywy o ochronie danych w sprawach karnych oraz do wszczynania postępowania sądowego lub udziału w postępowaniu sądowym w inny sposób. Uprawnienie to jest ważne i stanowi uzupełnienie innych środków, którymi dysponują organy nadzorujące ochronę danych, służących zapewnieniu wysokiego poziomu ochrony praw podstawowych osób fizycznych, a w szczególności ich prawa do ochrony ich danych osobowych.

2.2.3 Środki zaradcze

Wszystkie państwa członkowskie przewidziały prawo wniesienia skargi do odpowiedniego organu nadzorczego[56]. W większości przepisów prawa krajowego przewidziano określony termin na wniesienie tego rodzaju skargi. Ważne jest, aby to ograniczenie czasowe nie utrudniało osobom, których dotyczą dane, korzystania z ich praw.

Zgodnie z dyrektywą o ochronie danych w sprawach karnych[57] wszystkie państwa członkowskie przewidują środek prawny przed sądem od decyzji organu nadzorczego, z zastrzeżeniem innych środków administracyjnych lub pozasądowych środków ochrony prawnej dostępnych w ramach ich systemów prawnych. Środek prawny przed sądem jest dostępny we wszystkich państwach członkowskich, z wyjątkiem dwóch państw członkowskich[58], w których organ nadzorczy nie rozpatruje skargi ani nie informuje osób, których dane dotyczą, o postępach lub wynikach skargi w terminie 3 miesięcy[59].

Większość państw członkowskich przewiduje również środek prawny przed administratorem danych oraz podmiotem przetwarzającym dane[60] w przypadku domniemanego naruszenia dyrektywy o ochronie danych w sprawach karnych. W szeregu krajowych przepisów

[55] Taką możliwość przewidziało 18 państw członkowskich: Bułgaria, Czechy, Estonia, Grecja, Chorwacja, Włochy, Cypr, Litwa, Łotwa, Luksemburg, Węgry, Malta, Niderlandy, Austria, Portugalia, Rumunia, Słowacja i Szwecja. Organy nadzorujące ochronę danych w trzech państwach członkowskich (Estonia, Łotwa i Austria) mogą nakładać kary pieniężne na osoby fizyczne (np. pracowników) lub podmioty prywatne (np. podmioty prywatne przetwarzające dane).
[56] Art. 52 dyrektywy o ochronie danych w sprawach karnych.
[57] Art. 53 dyrektywy o ochronie danych w sprawach karnych.
[58] Finlandia i Szwecja.
[59] Art. 53 ust. 2 dyrektywy o ochronie danych w sprawach karnych.
[60] Art. 54 dyrektywy o ochronie danych w sprawach karnych.

transponujących nie przewiduje się jednak prawa osoby, której dane dotyczą, do upoważnienia organów, organizacji i zrzeszeń o charakterze niezarobkowym do złożenia skargi do organu nadzorczego lub wniesienia środka prawnego do sądu w jej imieniu[61].

2.2.4 Terminy przechowywania i przeglądu

Podejścia państw członkowskich do transpozycji przewidzianych w dyrektywie o ochronie danych w sprawach karnych terminów przechowywania i przeglądu danych osobowych[62] znacznie się od siebie różnią. Większość krajowych aktów prawnych dotyczących ochrony danych, które transponują dyrektywę o ochronie danych w sprawach karnych, spełnia jedynie ogólny wymóg art. 5 dyrektywy o ochrony danych w sprawach karnych. Oznacza to, że ustanowienie terminów usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych leży w gestii prawa sektorowego. Kilka państw członkowskich transponuje ten przepis, ustanawiając terminy w ustawodawstwie sektorowym.

W niektórych państwach członkowskich prawo pozostawia jednak ustalenie terminów właściwym organom. W niektórych przypadkach w przepisach nie określono żadnych kryteriów okresowego przeglądu ani nie zawarto w nich wymogu określenia takich kryteriów w innych przepisach, lub też nie przewidziano ustanowienia w prawie krajowym procedur mających na celu zapewnienie przestrzegania terminów.

Należy zauważyć, że bułgarski Naczelny Sąd Administracyjny zwrócił się niedawno do TSUE o udzielenie odpowiedzi na wniosek o wydanie orzeczenia w trybie prejudycjalnych dotyczący interpretacji art. 5 dyrektywy o ochronie danych w sprawach karnych w zakresie terminów przechowywania danych[63].

2.2.5 Podstawa prawna przetwarzania danych osobowych, w tym ich szczególnych kategorii

Większość państw członkowskich przewiduje, używając sformułowań, które często ściśle odpowiadają art. 8 dyrektywy ochronie danych w sprawach karnych, że podstawa prawna przetwarzania musi być określona w prawie unijnym lub prawie państwa członkowskiego. Niektóre krajowe akty prawne dotyczące ochrony danych osobowych transponujące dyrektywę o ochronie danych w sprawach karnych nie odzwierciedlają jednak wymogu, zgodnie z którym dane osobowe, które podlegają przetwarzaniu, oraz cele przetwarzania powinny być określone w przepisach prawa[64]. Z kolei inne krajowe akty prawne dotyczące ochrony danych osobowych transponujące dyrektywę o ochronie danych w sprawach karnych nie zawierają wszystkich przepisów odpowiadających art. 8. Określenie podstawy przetwarzania danych i spełnienie wymogów art. 8 należy do ustawodawstwa krajowego. Co więcej, samo powtórzenie ogólnych

[61] Art. 55 dyrektywy o ochronie danych w sprawach karnych.
[62] Art. 5 dyrektywy o ochronie danych w sprawach karnych.
[63] Wniosek o wydanie orzeczenia w trybie prejudycjalnym NG/Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR - Sofia, C-118/22.
[64] Art. 8 ust. 2 dyrektywy o ochronie danych w sprawach karnych.

wymogów art. 8 dyrektywy o ochronie danych w sprawach karnych w prawie krajowym nie może być uznane za wystarczającą podstawę prawną dla określonej operacji przetwarzania: w prawie krajowym należy określić, który organ jest właściwy do przetwarzania danych osobowych, jakie zadania publiczne, uzasadniające takie przetwarzanie, wykonuje oraz jaki jest cel przetwarzania.

Jeżeli chodzi o przetwarzanie szczególnych kategorii danych osobowych[65], większość państw członkowskich wymaga ścisłej konieczności jako warunku wstępnego przetwarzania danych. Większość państw członkowskich zapewnia również te same podstawy prawne do przetwarzania danych wrażliwych, które zostały określone w art. 10 dyrektywy o ochronie danych w sprawach karnych (przetwarzanie dopuszczone prawem; niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; dotyczące danych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą). W kilku państwach członkowskich w przepisach transponujących przewidziano pewne dodatkowe podstawy przetwarzania danych (np. gdy przetwarzanie takich danych jest konieczne, by zażegnać niebezpieczeństwo, które bezpośrednio zagraża życiu, integralności fizycznej lub mieniu osób, lub by zapobiec takiemu niebezpieczeństwu bądź by chronić zdrowie lub interesy osoby, której dane dotyczą, lub innej osoby). Jeżeli krajowy akt prawny o ochronie danych osobowych transponujący dyrektywę o ochronie danych w sprawach karnych nie zapewnia niezbędnych zabezpieczeń praw i wolności osób, których dane dotyczą (co ma miejsce w niektórych państwach członkowskich), należy uwzględnić takie zabezpieczenia w przepisach sektorowych.

Kilka krajowych przepisów transponujących odnosi się do zgody w odniesieniu do przetwarzania danych osobowych, w tym przetwarzania szczególnych kategorii danych osobowych. Należy pamiętać, że chociaż państwa członkowskie nie są pozbawione możliwości zapewnienia w swoim prawie krajowym, że osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie swoich danych osobowych do celów dyrektywy o ochronie danych w sprawach karnych, zgoda ta może służyć wyłącznie jako zabezpieczenie i nie może stanowić podstawy prawnej takiego przetwarzania. Dyskusje na ten temat wskazują, że wskazane byłoby wydanie bardziej szczegółowych wytycznych dotyczących roli zgody w kontekście przetwarzania danych osobowych do celów ścigania przestępstw.

2.2.6 Zautomatyzowane podejmowanie decyzji

Przepisy transponujące wszystkich państw członkowskich obejmują przepisy zakazujące podejmowania decyzji wyłącznie na podstawie zautomatyzowanego przetwarzania, jeżeli nie przewiduje tego prawo[66]. W przepisach transponujących większości państw członkowskich zawarto wymóg, by nie podejmować takich decyzji na podstawie szczególnych kategorii danych osobowych, chyba że zapewniono odpowiednie zabezpieczenia[67]. Zabroniono w nich także profilowania, które prowadzi do dyskryminacji[68]. Niektóre przepisy krajowe nie odwołują się jednak do odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą,

[65] Art. 10 dyrektywy o ochronie danych w sprawach karnych.
[66] Art. 11 ust. 1 dyrektywy o ochronie danych w sprawach karnych.
[67] Art. 11 ust. 2 dyrektywy o ochronie danych w sprawach karnych.
[68] Art. 11 ust. 3 dyrektywy o ochronie danych w sprawach karnych.

w przypadkach, gdy zautomatyzowane podejmowanie decyzji jest dozwolone przez prawo. W szczególności nie wszystkie państwa członkowskie przewidują prawo do uzyskania interwencji ludzkiej ze strony administratora lub wymagają odpowiednich środków zabezpieczających prawa lub wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą.

2.2.7 Prawa osoby, której dane dotyczą

Wszystkie państwa członkowskie postanowiły skorzystać z możliwości, jakie daje dyrektywa o ochronie w sprawach karnych, w zakresie ograniczenia prawa dostępu osób, których dane dotyczą, do ich danych osobowych[69]. Większość państw członkowskich przewiduje także ograniczenia innych praw osób, których dane dotyczą[70]. Krajowe akty prawne dotyczące ochrony danych, które transponują dyrektywę o ochronie danych w sprawach karnych, często posługują się jedynie ogólnym językiem dyrektywy o ochronie danych w sprawach karnych, nie określając bliżej okoliczności ani warunków, w których ograniczenia te mają być stosowane. W takich przypadkach okoliczności i warunki, o których mowa, muszą być określone w przepisach sektorowych; w przeciwnym przypadku administratorzy danych mieliby swobodę w stosowaniu tych ograniczeń.

Większość państw członkowskich spełnia określony w dyrektywie o ochronie danych w sprawach karnych wymóg, zgodnie z którym należy umożliwić osobom, których dane dotyczą, wykonywanie własnych praw za pośrednictwem organu nadzorującego ochronę danych[71]. Większość państw członkowskich skorzystała z możliwości postanowienia, że prawa osób, których dane dotyczą, należy wykonywać zgodnie z prawem krajowym w kontekście krajowego postępowania przygotowawczego lub sądowego w sprawie karnej[72].

Przepisy transponujące kilku państw członkowskich nie odzwierciedlają wszystkich szczególnych wymogów dyrektywy o ochronie danych w sprawach karnych dotyczących sposobu wykonywania praw osób, których dane dotyczą (np. formatu i sposobu przekazywania odpowiedzi, braku opłat).

Obecnie na rozpatrzenie oczekuje wniosek o wydanie orzeczenia w trybie prejudycjalnym [73]wniesiony przez niemiecki sąd w sprawie interpretacji ograniczenia praw dostępu osób, których dane dotyczą, do ich danych (art. 15 dyrektywy o ochronie danych w sprawach karnych w świetle art. 54 dyrektywy o ochronie danych w sprawach karnych), a także prawa do skutecznego środka prawnego przed sądem na mocy art. 47 Karty praw podstawowych oraz wolności wyboru zawodu na podstawie art. 15 Karty praw podstawowych.

[69] Art. 15 ust. 1 dyrektywy o ochronie danych w sprawach karnych.
[70] Art. 13 ust. 3 i art. 16 ust. 4.
[71] Art. 17 dyrektywy o ochronie danych w sprawach karnych.
[72] Art. 18 dyrektywy o ochronie danych w sprawach karnych.
[73]Wniosek o wydanie orzeczenia w trybie prejudycjalnym w sprawie TX/Bundesrepublik Deutschland, C-481/21.

2.2.8 Niektóre ważne przepisy specyficzne dla dyrektywy o ochronie danych w sprawach karnych

Niektóre przepisy dyrektywy o ochronie danych w sprawach karnych mają szczególne zastosowanie w kontekście ścigania przestępstw i nie mają swojego odpowiednika w RODO.

Kategorie osób, których dane dotyczą

W dyrektywie o ochronie danych w sprawach karnych nakłada się na państwa członkowskie obowiązek wymagania od administratora danych, by w stosownych przypadkach wyraźnie rozróżniał dane osobowe różnych kategorii osób oraz podawał przykłady tych kategorii (np. osoba, w stosunku do której istnieją poważne podstawy, by przypuszczać, że popełniła lub zamierza popełnić czyn zabroniony – „podejrzany")[74]. W przepisach niektórych państw członkowskich nie określono (w pewnym zakresie lub w ogóle) kategorii wymienionych w dyrektywie o ochronie danych w sprawach karnych. W odniesieniu do określenia kategorii „podejrzanych" niektóre przepisy krajowe nie wymagają, aby istniały „poważne podstawy, by przypuszczać, że [osoby te] popełniły lub zamierzają popełnić czyn zabroniony". Mające ukazać się wkrótce orzeczenie TSUE w toczącej się sprawie Ministerstvo na vatreshnite raboti przeciwko B.C. przyczyni się do dalszego wyjaśnienia wykładni dyrektywy o ochronie danych w sprawach karnych w odniesieniu do kategorii osób, których dane dotyczą, w tym wymogu, że zakwalifikowanie osoby, której dane dotyczą, jako podejrzanego powinno być uzależnione od istnienia „poważnych podstaw, by przypuszczać, że popełniła ona lub zamierza popełnić czyn zabroniony"[75].

Rozróżnienie klas danych osobowych oraz weryfikacja ich jakości

Państwa członkowskie muszą zapewnić, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe, od danych osobowych opartych na indywidualnych ocenach[76]. Muszą także wprowadzić odpowiednie środki, aby zapewnić, by nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane ani udostępniane. W przypadku przekazania nieprawidłowych danych należy niezwłocznie powiadomić odbiorców, a następnie sprostować dane osobowe, usunąć je lub ograniczyć ich przetwarzanie. Chociaż większość państw członkowskich dokonała transpozycji tego wymogu, w szeregu krajowych przepisów transponujących nie przewidziano wyraźnie niektórych wymaganych środków szczególnych.

Ewidencja czynności

[74] Art. 6 dyrektywy o ochronie danych w sprawach karnych.
[75] Wniosek o wydanie orzeczenia w trybie prejudycjalnym w sprawie Ministerstvo na vatreshnite raboti/ B.C., C-205/21.
[76] Art. 7 dyrektywy o ochronie danych w sprawach karnych.

Łącznie 12 państw członkowskich[77] skorzystało z możliwości odroczenia dostosowania swojego systemu automatycznego przetwarzania danych do wymogów dotyczących prowadzenia ewidencji czynności do maja 2023 r.[78]

Większość państw członkowskich przewiduje prowadzenie ewidencji czynności przetwarzania w systemach automatycznego przetwarzania danych[79]. Niektóre przepisy prawa krajowego nie przewidują wymogu prowadzenia ewidencji wszystkich rodzajów czynności. W dyrektywie o ochronie danych w sprawach karnych określono minimalny zakres informacji, które należy ewidencjonować. W niektórych przepisach prawa krajowego nie uwzględniono wszystkich wymaganych rodzajów informacji (np. powodu przeglądania lub ujawniania danych osobowych).

3 PIERWSZE WNIOSKI ZE STOSOWANIA I FUNKCJONOWANIA DYREKTYWY O OCHRONIE DANYCH W SPRAWACH KARNYCH

3.1 Skargi oraz pozytywny wpływ na prawa osób, których dane dotyczą

Dyrektywa o ochronie danych w sprawach karnych zapewnia ochronę podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych. Stanowi wszechstronne ramy dla praw osoby, której dane dotyczą, oraz sposobu wykonywania tych praw, w tym prawa do informacji, dostępu, sprostowania lub usunięcia danych osobowych, jak również prawa do ograniczenia ich przetwarzania. Dyrektywa o ochronie danych w sprawach karnych zwiększyła wśród osób, których dane dotyczą, zrozumienie ich praw oraz sposobów ich wykonywania, o czym świadczy wzrost liczby wniosków składanych do właściwych organów. Praktyka pokazuje, że spośród praw przyznanych osobom, których dane dotyczą, na podstawie dyrektywy o ochronie danych w sprawach karnych, to właśnie wnioski dotyczące prawa dostępu do danych oraz prawa do ich usunięcia są najczęściej składane we właściwych organach[80].

Dyrektywa o ochronie danych w sprawach karnych umożliwia również ograniczenie niektórych praw (prawo dostępu[81] i prawo do sprostowania lub usunięcia[82]), a także informacji, które administrator danych musi przekazać osobie, której dane dotyczą, w odniesieniu do danych osobowych będących przedmiotem przetwarzania[83]. Osoby, których dane dotyczą, mogą zwrócić się do organów nadzorujących ochronę danych o dokonanie przeglądu ograniczenia danego prawa przez właściwy organ lub o sprawdzenie, czy ograniczenie zostało zastosowane zgodnie z dyrektywą o ochronie danych w sprawach karnych (pośrednie wykonywanie prawa)[84]. Blisko

[77] Niemcy skorzystały z tej opcji w przypadku niektórych ustaw transponujących dyrektywę o ochronie danych w sprawach karnych na szczeblu federalnym i krajów związkowych.
[78] Art. 63 ust. 2 dyrektywy o ochronie danych w sprawach karnych.
[79] Art. 25 dyrektywy o ochronie danych w sprawach karnych.
[80] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 15.
[81] Art. 15 dyrektywy o ochronie danych w sprawach karnych.
[82] Art. 16 dyrektywy o ochronie danych w sprawach karnych.
[83] Art. 13 dyrektywy o ochronie danych w sprawach karnych.
[84] Art. 17 dyrektywy o ochronie danych w sprawach karnych.

połowa organów nadzorujących ochronę danych zgłasza, że otrzymała wniosek tego rodzaju[85]. Praktyka pokazuje, że liczba otrzymanych wniosków może się znacznie różnić (np. w Chorwacji otrzymano jeden taki wniosek, a we Francji otrzymano ich ponad 1500)[86]. Choć organy nadzorujące ochronę danych ustaliły w wyniku weryfikacji lub przeglądu tych skarg, że większość wniosków była niedopuszczalna, w kilku przypadkach administratorowi danych nakazano sprostowanie lub usunięcie danych osobowych lub ograniczenie ich przetwarzania, zapewniając w ten sposób właściwe stosowanie ograniczeń[87].

W dyrektywie o ochronie danych w sprawach karnych przewidziano, że organ, organizacja lub zrzeszenie o charakterze niezarobkowym mogą złożyć skargę w imieniu osoby, której dane dotyczą. Wydaje się jednak, że zapis ten nie jest w pełni wykorzystywany (tylko cztery organy nadzorujące ochronę danych zgłosiły, że otrzymały taką skargę od organu przedstawicielskiego[88]). Podobnie organizacje społeczeństwa obywatelskiego zgłosiły, że otrzymały niewielką liczbę wniosków o złożenie tego rodzaju skargi[89].

Osoby fizyczne również w coraz większym stopniu korzystają z przysługującego im prawa do wniesienia skargi do organów nadzorujących ochronę danych, w tym w przypadkach gdy właściwe organy ograniczają wykonywanie praw osób, których dane dotyczą. Ponad jedna trzecia organów nadzorujących ochronę danych zgłosiła wzrost liczby otrzymywanych skarg po transpozycji dyrektywy o ochronie danych w sprawach karnych w swoich państwach członkowskich[90]. Niektóre ze skarg najczęściej otrzymywanych przez organy nadzorujące ochronę danych dotyczyły ograniczenia prawa dostępu[91], prawa do sprostowania lub usunięcia[92] oraz prawa do informacji i jego ograniczeń[93]. Następnie pojawiły się skargi związane z zasadą ograniczenia przechowywania, która zobowiązuje właściwe organy do przechowywania danych osobowych przez okres nie dłuższy niż jest to konieczne, oraz z prawem do informacji.

3.2 Zwiększona świadomość w zakresie ochrony danych wśród właściwych organów

Państwa członkowskie wskazują, że wprowadzenie dyrektywy o ochronie danych w sprawach karnych wywarło i nadal wywiera znaczący wpływ na świadomość właściwych organów w zakresie znaczenia ochrony danych[94]. Kilka organów nadzorujących ochronę danych wyraziło

---

[85] Cztery organy nadzorujące ochronę danych nie prowadzą statystyk dotyczących wniosków otrzymanych na podstawie art. 17 dyrektywy o ochronie danych w sprawach karnych.
[86] Dotyczą one wniosków złożonych od momentu transpozycji dyrektywy o ochronie danych w sprawach karnych do grudnia 2021 r. Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych (indywidualne odpowiedzi organów ochrony danych).
[87] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 50.
[88] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 33.
[89] Trzy organizacje (w kontekście odpowiedzi na kwestionariusze przesłane im przez Agencję Praw Podstawowych) zgłosiły, że otrzymały jeden wniosek, a jedna organizacja zgłosiła, że otrzymała więcej wniosków niż jeden.
[90] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 31.
[91] Art. 15 dyrektywy o ochronie danych w sprawach karnych.
[92] Art. 16 dyrektywy o ochronie danych w sprawach karnych.
[93] Art. 13 dyrektywy o ochronie danych w sprawach karnych.
[94] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 21.

opinię, że najważniejszym skutkiem dyrektywy o ochronie danych w sprawach karnych było zwiększenie świadomości i nacisku na kwestie ochrony danych i praw osób, których dane dotyczą[95]. Świadczy o tym również wymiana informacji między organami nadzorującymi ochronę danych a właściwymi organami na temat praw osób, których dane dotyczą, oraz sposobów korzystania z tych praw[96]. Niektóre właściwe organy poinformowały, że w konsekwencji przeznaczyły więcej zasobów na ochronę danych[97]. Obejmowało to inwestycje w uwzględnienie ochrony prywatności już w fazie projektowania i w sposób domyślny w ich systemach informatycznych, ustanowienie okresów zatrzymywania danych, stosowanie zasady minimalizacji danych oraz zgłaszanie naruszeń. Następnie zgłoszono poprawę ogólnego bezpieczeństwa przetwarzanych danych[98].

Prowadzone przez organy nadzorujące ochronę danych szkolenia i działania zwiększające świadomość również przyczyniają się do właściwego wdrożenia dyrektywy o ochronie danych w sprawach karnych, a organy nadzorcze mają za zadanie zwiększać świadomość administratorów danych i podmiotów przetwarzających dane w zakresie ich obowiązków wynikających z dyrektywy o ochronie danych w sprawach karnych[99].

Wiele organów nadzorujących ochronę danych stara się zwiększać świadomość w zakresie ochrony danych, publikując odpowiednie wytyczne. Niektóre z tematów poruszanych przez różne organy nadzorujące ochronę danych obejmują: wsparcie organów sądowniczych, prokuratury oraz służb policji w przestrzeganiu zasady rozliczalności; wymianę danych osobowych z policją; powołanie inspektora ochrony danych; prowadzenie oceny skutków dla ochrony danych; przetwarzanie danych w takich dziedzinach przestępczości jak przestępczość zorganizowana i terroryzm; rejestrowanie i ewidencjonowanie czynności przetwarzania; prowadzenie monitoringu wizyjnego; przekazywanie informacji osobom, których dane dotyczą; zgłaszanie naruszeń ochrony danych osobowych; obowiązki administratora oraz wykonywanie praw przez osoby fizyczne.

Osiem organów nadzorujących ochronę danych nie wydało jednak jeszcze żadnych wskazówek ani praktycznych narzędzi mających na celu wsparcie właściwych organów i podmiotów przetwarzających w wypełnianiu ich obowiązków.

Co więcej, 12 organów nadzorujących ochronę danych nie przeprowadziło w ramach dyrektywy o ochronie danych w sprawach karnych żadnych szkoleń ani działań zwiększających świadomość skierowanych do właściwych organów lub podmiotów przetwarzających[100]. Wśród organów

---

[95] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych (indywidualne odpowiedzi organów ochrony danych).
[96] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 40 oraz stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, s. 9.
[97] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 70.
[98] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 70.
[99] Art. 46 ust. 1 lit. d) dyrektywy o ochronie danych w sprawach karnych.
[100] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych (indywidualne odpowiedzi organów ochrony danych).

nadzorujących ochronę danych, które prowadziły takie działania, do najczęściej poruszanych tematów należały: przetwarzanie danych przez policję, prokuraturę, organy sądowe oraz władze penitencjarne; określenie odpowiednich obszarów zastosowania RODO i dyrektywy o ochronie danych w sprawach karnych; wykorzystanie danych osobowych pochodzących z mediów społecznościowych; przetwarzanie danych zawartych w aktach policyjnych; techniki monitoringu wizyjnego i duże zbiory danych; sposób postępowania w odniesieniu do praw osoby, której dane dotyczą oraz przetwarzanie danych osobowych osób pozbawionych wolności[101].

Kolejną innowacją wprowadzoną dyrektywą o ochronie danych w sprawach karnych jest wymóg wyznaczenia przez administratorów danych inspektora ochrony danych, do którego obowiązków należy m.in.: informowanie i doradzanie w zakresie wymogów ochrony danych, monitorowanie zgodności z dyrektywą o ochronie danych w sprawach karnych, doradzanie w zakresie ocen skutków dla ochrony danych oraz monitorowanie ich wykonywania[102]. Dzięki temu rozwiązaniu właściwe organy stały się bardziej świadome swoich obowiązków w zakresie ochrony danych. Miało ono także pozytywny wpływ na przestrzeganie przez właściwe organy zasad ochrony danych, co odnotowała również Rada[103].

Ważne jest, aby inwestować w rozwój oraz poszerzanie doświadczenia i wiedzy inspektorów ochrony danych, aby pomóc właściwym organom w spójnym stosowaniu dyrektywy o ochronie danych w sprawach karnych[104]. W związku z tym Komisja ustanowiła sieć inspektorów ochrony danych właściwych organów, agencji wymiaru sprawiedliwości i spraw wewnętrznych oraz Prokuratury Europejskiej i wspomaga działanie tej sieci. Sieć ta jest stałą inicjatywą, skupiająca się na stosowaniu dyrektywy o ochronie danych w sprawach karnych przez właściwe organy państw członkowskich. Ma ona na celu stworzenie platformy współpracy i wymiany wiedzy eksperckiej między inspektorami ochrony danych z poszczególnych państw członkowskich. Sieć ekspertów ds. ochrony danych Europolu i krajowe sieci inspektorów ochrony danych działające w ramach właściwych organów stanowią ważne inicjatywy pomagające inspektorom ochrony danych działającym w ramach właściwych organów wspierać wymianę najlepszych praktyk i informacji na temat stosowania dyrektywy o ochronie danych w sprawach karnych.

3.3 Bezpieczeństwo danych zwiększyło się, choć występują rozbieżności w zakresie powiadomień o naruszeniu ochrony danych

Dyrektywa o ochronie danych w sprawach karnych przyczyniła się do poprawy bezpieczeństwa danych osobowych dzięki zobowiązaniu właściwych organów do podjęcia działań służących osiągnięciu określonych celów w zakresie bezpieczeństwa. Przykładowo, w dyrektywie zawarto wymóg, aby właściwe organy przeprowadzały ocenę skutków dla ochrony danych, gdy przetwarzanie może powodować wysokie ryzyko dla praw i wolności osoby, której dane dotyczą. Ocena skutków obejmuje identyfikację ryzyka oraz środków mających na celu przeciwdziałanie

[101] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 41–42.
[102] Art. 32–34 dyrektywy o ochronie danych w sprawach karnych.
[103] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 22.
[104] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 25.

temu ryzyku. Wymóg ten, jak również obowiązkowe przestrzeganie zasady uwzględniania ochrony danych już w fazie projektowania i w sposób domyślny oraz wymogi dotyczące zgłaszania naruszeń ochrony danych osobowych, przyczynił się do poprawy bezpieczeństwa przetwarzania danych osobowych[105].

Dostrzegła to również Rada, stwierdzając, że dzięki dyrektywie o ochronie danych w sprawach karnych nastąpiła poprawiła poziomu bezpieczeństwa danych, między innymi dzięki sporządzaniu planów bezpieczeństwa; aktualizacji systemów informatycznych oraz środków organizacyjnych; prowadzeniu ocen skutków dla ochrony danych oraz wymogowi prowadzenia ewidencji określonych czynności przetwarzania przez właściwe organy[106].

W dyrektywie o ochronie danych w sprawach karnych określono okoliczności, w których administratorzy danych muszą powiadomić swój organ nadzorujący ochronę danych oraz osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych[107]. Pomimo tego obowiązku istnieje duża rozbieżność w liczbie naruszeń ochrony danych, które zostały zgłoszone organom nadzorujących ochronę danych od czasu wprowadzenia dyrektywy[108]. Sześć organów nadzorujących ochronę danych poinformowało, że nie otrzymały żadnych powiadomień o naruszeniu ochrony danych[109], a szereg innych zgłosiło, że otrzymało bardzo niewielką liczbą takich powiadomień. Przykładowo organ włoski zgłosił tylko trzy powiadomienia o naruszeniu ochrony danych, organ francuski – osiem, natomiast organ holenderski – ponad 500.

Ta różnica w liczbie zgłoszonych powiadomień o naruszeniu ochrony danych wskazuje (po uwzględnieniu czynników takich jak wielkość populacji), że między właściwymi organami państw członkowskich mogą istnieć rozbieżne praktyki dotyczące tego, co uznaje się za naruszenie i kiedy należy je zgłosić organowi nadzorującemu ochronę danych. Komisja zwróciła na to również uwagę w swoim sprawozdaniu w sprawie RODO[110]. EROD opublikowała niedawno wytyczne dotyczące naruszeń w ramach RODO[111]. Wytyczne te, choć nie mają bezpośredniego zastosowania, mają również znaczenie w przypadku naruszeń ochrony danych w związku z dyrektywą o ochronie danych w sprawach karnych. Powinny zatem przyczynić się do bardziej

---

[105] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 70 i 71 oraz indywidualne odpowiedzi inspektorów ochrony danych (Niemcy, Finlandia, Francja, Węgry, Malta).
[106] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 26.
[107] Art. 30 i 31 dyrektywy o ochronie danych w sprawach karnych.
[108] Dane liczbowe obejmują wszystkie naruszenia ochrony danych zgłoszone w okresie od transpozycji dyrektywy o ochronie danych w sprawach karnych do grudnia 2021 r. Dane zebrano od organów nadzorujących ochronę danych osobowych w grudniu 2021 r.
[109] Hiszpania, Chorwacja, Litwa, Portugalia, Słowacja i Słowenia.
[110] Dokument roboczy służb Komisji, Komunikatu Komisji do Parlamentu Europejskiego i Rady pt.: „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych", COM(2020) 264 final.
[111] Wytyczne EROD z 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych, przyjęte 14 grudnia 2021 r., https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

jednolitego podejścia do postępowania w przypadku naruszeń ochrony danych w związku z dyrektywą o ochronie danych w sprawach karnych we wszystkich państwach członkowskich.

3.4 Nadzór sprawowany przez organy nadzorujące ochronę danych

3.4.1 Zasoby organów nadzorujących ochronę danych

Zapewnienie każdemu organowi ochrony danych zasobów kadrowych, technicznych i finansowych, pomieszczeń i infrastruktury jest warunkiem koniecznym skutecznego wypełniania przez nie ich zadań i wykonywania ich uprawnień, a zatem stanowi podstawowy warunek ich niezależności[112]. Komisja konsekwentnie podkreślała fakt, że państwa członkowskie są zobowiązane do przydzielenia organom nadzorującym ochronę danych wystarczających zasobów ludzkich, finansowych i technicznych[113]. Rada również wyraźnie wezwała państwa członkowskie do przydzielenia organom nadzorującym ochronę danych wystarczających zasobów ludzkich, technicznych i finansowych[114].

Wydaje się jednak, że ogólny wzrost liczby pracowników organów nadzorujących ochronę danych w ostatnich latach[115] nie ma związku z zadaniami wynikającymi z dyrektywy o ochronie danych w sprawach karnych. Połowa organów nadzorujących ochronę danych utrzymała tę samą liczbę pracowników zajmujących się dyrektywą o ochronie danych w sprawach karnych lub nawet obniżyła poziom zatrudnienia w tym zakresie[116]. Wszelkie wzrosty były bardzo nieznaczne i wynosiły średnio mniej niż dwie osoby w przeliczeniu na ekwiwalenty pełnego czasu pracy[117]. W niemal połowie organów nadzorujących ochronę danych (w tym w tych zatrudniających ponad 100 pracowników w przeliczeniu na ekwiwalenty pełnego czasu pracy) liczba pracowników zajmujących się dyrektywą o ochronie danych w sprawach karnych waha się od mniej niż 1 % do 7 %[118]. W liczbach bezwzględnych około połowa organów nadzorujących ochronę danych przeznacza na zadania związane z dyrektywą o ochronie danych w sprawach karnych od 1 do 4 ekwiwalentów pełnego czasu pracy, a osiem organów nadzorujących ochronę danych przeznacza

---

[112] Art. 42 ust. 4 dyrektywy o ochronie danych w sprawach karnych.
[113] Komunikat Komisji do Parlamentu Europejskiego i Rady „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych", COM(2020) 264 final.
[114] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 12.
[115] Wkład EROD w ocenę ogólnego rozporządzenia o ochronie danych na podstawie art. 97, 18 lutego 2020 r., s. 26–29.
https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf
Przegląd EROD dotyczący zasobów udostępnianych przez państwa członkowskie organom ochrony danych oraz działań organów ochrony danych w zakresie egzekwowania przepisów („przegląd EROD dotyczący zasobów"), 5 sierpnia 2021 r., s. 4–5.
https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_en
[116] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 65 i wykres w pytaniu 41, s. 20.
[117] Niemcy wskazały na znaczny wzrost z 33 do 53 ekwiwalentów pełnego czasu pracy w okresie od 2017 do 2021 r.
[118] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, wykres w pytaniu 41, s. 20. Przegląd EROD dotyczący zasobów, s. 5.

na zadania związane z tą dyrektywą od 7 do 15 ekwiwalentów pełnego czasu pracy. Jeden organ nadzorujący ochronę danych zatrudnia jednak 53 pracowników zajmujących się tą dyrektywą – w przeliczeniu na ekwiwalenty pełnego czasu pracy[119]. Jednocześnie sekretariat EROD przeznaczył mniej niż 1,5 ekwiwalentu pełnego czasu pracy na kwestie całkowicie związane z dyrektywą o ochronie danych w sprawach karnych.

Sytuacja ta nie jest zadowalająca, nawet jeśli 10 organów nadzorujących ochronę danych wskazało, że dysponują wystarczającymi zasobami finansowymi, ludzkimi i technicznymi[120]. Z drugiej strony 16 organów nadzorujących ochronę danych stwierdziło, że nie dysponują wystarczającymi zasobami. Niektóre z tych organów zauważyły, że miało to negatywny wpływ na dochodzenia prowadzone przez nie z własnej inicjatywy[121], rozpatrywanie skarg[122], kontrolę wielkoskalowych systemów informatycznych oraz wydawanie opinii z własnej inicjatywy[123]. Specyfika sektora wiąże się bowiem z tym, że skuteczne egzekwowanie dyrektywy o ochronie danych w sprawach karnych wymaga systematycznej kontroli czynności przetwarzania, które często są złożone, i że nie wystarczy polegać na indywidualnych skargach (których liczba jest znacznie mniejsza niż w przypadku RODO)[124].

Co więcej, organy nadzorujące ochronę danych wskazały na brak wiedzy specjalistycznej w zakresie technologii informatycznych, która pozwoliłaby uwzględnić stale rosnącą złożoność technologii informatycznych wykorzystywanych w obszarze ścigania przestępstw[125].

3.4.2 Korzystanie z uprawnień

Korzystanie z uprawnień naprawczych

Łącznie 19 organów nadzorujących ochronę danych zastosowało swoje uprawnienia w zakresie prowadzenia postępowań, z inicjatywy własnej lub w odpowiedzi na otrzymaną skargę[126]. Organy nadzorujące ochronę danych zgłosiły trudności jedynie w bardzo niewielu przypadkach (np. gdy

[119] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, wykres w pytaniu 41, s. 19.
[120] Belgia, Dania, Irlandia, Grecja, Łotwa, Luksemburg, Węgry, Malta, Austria i Finlandia.
[121] Niemcy i Francja.
[122] Francja i Szwecja.
[123] Niderlandy.
[124] Od 2018 r. Irlandia otrzymała 135 skarg związanych z dyrektywą o ochronie danych w sprawach karnych, a Węgry otrzymały 141 skarg, natomiast Dania otrzymała 223 skarg od 2017 r. Dla porównania złożono tysiące skarg związanych z RODO (zob. przegląd EROD dotyczący zasobów, s. 10).
[125] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 69.
[126] Organy nadzorujące ochronę danych w Irlandii, na Malcie i w Niderlandach poinformowały, że prowadziły dochodzenia z inicjatywy własnej. Organy nadzorujące ochronę danych w Grecji, Hiszpanii, na Litwie i Węgrzech przeprowadziły dochodzenia na podstawie otrzymanych skarg. Organy nadzorujące ochronę danych w Belgii, Bułgarii, Danii, Niemczech, Francji, Włoszech, Luksemburgu, Austrii, Polsce, Słowenii i Szwecji przeprowadziły dochodzenia zarówno z inicjatywy własnej, jak i w odpowiedzi na otrzymane skargi.

administrator danych nie dostarczył wszystkich istotnych informacji lub odmówił dostępu do informacji)[127].

Te same 19 organów nadzorujących ochronę danych zastosowało również swoje uprawnienia naprawcze. Zdecydowanie najczęściej wykorzystywanym uprawnieniem było wydawanie nakazów dostosowania przetwarzania do wymogów prawa, w tym nakazów sprostowania lub usunięcia danych osobowych bądź ograniczenia ich przetwarzania. Organy nadzorujące ochronę danych skorzystały z tego uprawnienia w 114 przypadkach. Fakt, że to uprawnienie do nakazania tymczasowego lub ostatecznego ograniczenia (w tym zakazu) przetwarzania danych zostało wykorzystane jedynie w czterech przypadkach[128], wskazuje, że organy nadzorujące ochronę danych korzystały z tych uprawnień z ostrożnością.

Korzystanie z uprawnień doradczych

Prowadzenie w sposób systematyczny uprzednich konsultacji i zwracanie się do organów nadzorujących ochronę danych o opinię na temat projektów środków legislacyjnych i administracyjnych stanowią skuteczny sposób zapewnienia wysokiego poziomu ochrony prawa do ochrony danych osobowych i zmniejszenia liczby kolejnych skarg. Uprzednie konsultacje z organami nadzorującymi ochronę danych mają szczególne znaczenie w przypadku stosowania nowych technologii, które mogą mieć istotny wpływ na prawa podstawowe.

Połowa organów nadzorujących ochronę danych podała, że skonsultowano z nimi oceny skutków dla ochrony danych. Liczba uprzednich konsultacji różni się między państwami członkowskimi. Do niektórych organów zwrócono się tylko raz, natomiast jeden z organów otrzymał 59 wniosków w sprawie uprzedniej konsultacji[129]. W większości tych przypadków organy nadzorujące ochronę danych udzieliły pisemnej porady, a w niektórych przypadkach skorzystały ze swoich uprawnień naprawczych w odniesieniu do przetwarzania danych, w szczególności wydały ostrzeżenia lub nakazały podjęcie działań w celu dostosowania przetwarzania do wymogów prawa. W jednym przypadku organ nadzorujący ochronę danych wydał negatywną opinię, która, jak się wydaje, miała taki sam skutek jak zakaz przetwarzania.

Co więcej, wydaje się, że poza procedurą uprzedniej konsultacji organy nadzorujące ochronę danych zajmują się również wnioskami o udzielenie porady. Najczęściej występujący problem, w sprawie którego właściwe organy zwracały się do organów nadzorujących ochronę danych o poradę, dotyczył konkretnych rodzajów przetwarzania (w szczególności stosowania nowych

[127] Niemieckie i węgierskie organy nadzorujące ochronę danych stwierdziły, że nie otrzymały wszystkich niezbędnych informacji lub że administrator odmówił im dostępu do niezbędnych informacji. Organy niemieckie wspomniały, że nie przewidziano uprawnienia podobnego do art. 58 ust. 1 lit. a) RODO.
[128] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 30 oraz indywidualne odpowiedzi organów z Austrii i Luksemburga.
[129] Organy nadzorujące ochronę danych z Danii i Litwy zgłosiły, że skonsultowano się z nimi tylko raz. Organ nadzorujący ochronę danych z Belgii otrzymał 59 wniosków w sprawie uprzedniej konsultacji.

technologii, mechanizmów lub procedur, a także odpowiednich środków bezpieczeństwa, przetwarzania szczególnych kategorii danych osobowych, określania podstawy prawnej przetwarzania, zasad ograniczenia przechowywania oraz odpowiednich terminów przechowywania[130]).

Co więcej, 22 organy nadzorujące ochronę danych skierowały do swoich parlamentów narodowych i rządów krajowych opinie w sprawie środków legislacyjnych i administracyjnych dotyczących przetwarzania danych osobowych. Szereg organów wskazało, że sporadycznie są proszone o konsultację[131].

3.4.3 Kontrola sądowa działania organów nadzorujących ochronę danych

Niemal połowa organów nadzorujących ochronę danych wskazała, że w niewielkiej liczbie przypadków wytoczono im postępowanie sądowe w związku z podjętymi przez nie decyzjami lub ich bezczynnością. W większości przypadków postępowania wszczęły osoby, których dane dotyczą, a w kilku przypadkach – właściwe organy[132]. Kilka spraw zostało uznanych przez sąd za niedopuszczalne lub wycofanych przez stronę skarżącą. Sąd podtrzymał decyzję organów nadzorujących ochronę danych w większości pozostałych spraw, ale uchylił ją w kilku sprawach (przy czym pozostałe postępowania nadal się toczą). W związku z niewielką liczbą wydanych do tej pory wyroków nie można jeszcze ustalić wyraźnej tendencji.

3.4.4 Wytyczne EROD

Spójność oraz wysoki poziom ochrony wśród państw członkowskich ma zasadnicze znaczenie dla zapewnienia skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy policyjnej[133]. W dyrektywie o ochronie danych w sprawach karnych przewidziano, że EROD wyda wytyczne, zalecenia i najlepsze praktyki (z własnej inicjatywy lub na wniosek Komisji), aby zapewnić spójne stosowanie dyrektywy o ochronie danych w sprawach karnych przez państwa członkowskie. EROD opracowała wytyczne dotyczące dyrektywy o ochronie danych w sprawach karnych odnoszące się do rozdziału V (międzynarodowe przekazywanie

[130] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 39.
[131] Organy nadzorujące ochronę danych w Czechach, Grecji, Chorwacji, Łotwie i Szwecji poinformowały, że nie wydały opinii. Organy nadzorujące ochronę danych w Grecji, Chorwacji, Łotwie, Polsce, Rumunii, Słowenii i Słowacji były proszone o konsultację tylko sporadycznie.
[132] Obserwacja ta opiera się na odpowiedziach otrzymanych od organów nadzorujących ochronę danych w Belgii, Bułgarii, Niemczech, Estonii, Irlandii, we Włoszech, na Węgrzech, w Niderlandach, Austrii, Polsce, Finlandii i Szwecji.
[133] Motyw 7 dyrektywy o ochronie danych w sprawach karnych.

danych)[134]; wytyczne dotyczące stosowania technologii rozpoznawania twarzy[135] oraz (pełniąc swoją poprzednią rolę Grupy Roboczej Art. 29) opinię w sprawie niektórych kluczowych kwestii dotyczących dyrektywy o ochronie danych w sprawach karnych[136].

Wiele wytycznych EROD dotyczących RODO ma również zastosowanie do dyrektywy o ochronie danych w sprawach karnych w zakresie, w jakim opierają się one na wspólnych koncepcjach lub technologiach. Wytyczne te obejmują wytyczne dotyczące koncepcji administratora danych i podmiotu przetwarzającego dane[137], praw osób, których dane dotyczą[138], zgłaszania naruszeń ochrony danych osobowych[139], oceny skutków dla ochrony danych[140], uwzględnienia ochrony danych już w fazie projektowania i w sposób domyślny[141] oraz indywidualnego zautomatyzowanego podejmowania decyzji[142].

Opracowanie kompleksowych i praktycznych wytycznych wymaga znacznego nakładu pracy i środków, ale wskazówki są niezbędne (co zauważyła również Rada[143]). W związku z tym bardzo cieszy, że EROD wskazała, iż wkrótce przedstawi dodatkowe wytyczne, w tym dotyczące pojęcia

---

[134] Zalecenia EROD z 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie dyrektywy o ochronie danych w sprawach karnych, przyjęte 2 lutego 2021 r. https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf

[135] Wytyczne EROD z 05/2022 w sprawie wykorzystania technologii rozpoznawania twarzy w obszarze ścigania przestępstw, przyjęte 12 maja 2022 r., wersja do konsultacji społecznych, dostępne pod adresem:https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

[136] Opinia Grupy Roboczej Art. 29 dotycząca niektórych głównych zagadnień dyrektywy (UE) 2016/680 dotyczącej egzekwowania prawa, plan prac 258, przyjęta 29 listopada 2017 r., dostępna na stronie: https://ec.europa.eu/newsroom/article29/items/612053/enhttps://ec.europa.eu/newsroom/article29/items/610178/en.

[137] Wytyczne EROD z 07/2020 dotyczące koncepcji administratora danych i podmiotu przetwarzającego dane, przyjęte 7 lipca 2021 r., dostępne pod adresem:https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

[138] Wytyczne EROD z 01/2022 dotyczące praw osób, których dane dotyczą – prawo dostępu, przyjęte 18 stycznia 2022 r., wersja do konsultacji społecznych, dostępne pod adresem:https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

[139] Wytyczne Grupy Roboczej Art. 29 w sprawie zgłaszania naruszeń ochrony danych osobowych na podstawie rozporządzenia 2016/679, plan prac 250rev.01, poddane ostatniemu przeglądowi 6 lutego 2018 r. i zatwierdzone przez EROD 25 maja 2018 r., dostępne na stronie: https://ec.europa.eu/newsroom/article29/items/612052/en; Wytyczne EROD z 01/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych, przyjęte 14 grudnia 2021 r., dostępne pod adresem:https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

[140] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, plan prac 248rev.01, poddane ostatniemu przeglądowi 4 października 2017 r. i zatwierdzone przez EROD 25 maja 2018 r., dostępne na stronie: https://ec.europa.eu/newsroom/article29/items/611236

[141] Wytyczne EROD z 4/2019 dotyczące ochrony danych w fazie projektowania oraz w sposób domyślny na podstawie art. 25, przyjęte 20 października 2020 r., dostępne pod adresem:https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[142] Wytyczne Grupy Roboczej Art. 29 w sprawie w sprawie zautomatyzowanego podejmowania decyzji indywidualnych i profilowania dla celów rozporządzenia 2016/679, plan prac 251rev.01, poddane ostatniemu przeglądowi 6 lutego 2018 r. i zatwierdzone przez EROD 25 maja 2018 r.; dostępne na stronie: https://ec.europa.eu/newsroom/article29/items/612053/en

[143] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 14.

skutecznych uprawnień w zakresie prowadzenia postępowań, a także uprawnień naprawczych organów nadzorujących ochronę danych i międzynarodowego przekazywania danych podlegającego odpowiednim zabezpieczeniom.

Wytyczne EROD mogą również przyczynić się do zmniejszenia obciążenia pracą organów nadzorujących ochronę danych (np. w odniesieniu do zadań takich, jak doradzanie administratorom danych lub rozpatrywanie skarg). Na przykład szereg kwestii poruszonych w opinii Grupy Roboczej Art. 29 na temat niektórych kluczowych zagadnień ujętych w dyrektywie o ochronie danych w sprawach karnych (takich jak odpowiednie terminy, podstawa prawna przetwarzania, warunki przetwarzania szczególnych kategorii danych) to również jedne z najczęstszych problemów, w sprawie których właściwe organy zwróciły się o poradę do organów nadzorujących ochronę danych[144].

3.4.5 Wzajemna pomoc

Aby zapewnić spójne stosowanie dyrektywy o ochronie danych w sprawach karnych, organy nadzorujące ochronę danych są zobowiązane do udzielania sobie wzajemnej pomocy. Obejmuje to pomoc w formie wniosków o udzielenie informacji oraz wniosków o przeprowadzenie konsultacji, inspekcji i dochodzeń[145]. Dotychczas jednak korzystano z wzajemnej pomocy bardzo rzadko. Skorzystało z niej zaledwie sześć organów nadzorujących ochronę danych, przede wszystkim w odpowiedzi na wnioski o udzielenie informacji otrzymane od innych organów nadzorujących ochronę danych. Większość organów nadzorujących ochronę danych wskazała, że otrzymała tylko jeden wniosek o udzielenie informacji. Wszystkie te organy poinformowały, że przychyliły się do otrzymanego wniosku. Nie korzystano także z dobrowolnej wzajemnej pomocy, w odniesieniu do której nie istnieją określone przepisami terminy ani wyraźny obowiązek odpowiedzi. EROD oświadczyła, że opublikuje wytyczne dotyczące ram wzajemnej pomocy na podstawie RODO i dyrektywy o ochronie danych w sprawach karnych[146].

3.5 Elastyczny instrument międzynarodowego przekazywania danych

Rozdział V dyrektywy o ochronie danych w sprawach karnych obejmuje przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych. Rozdział ten zasadniczo zapewnia ciągłość ochrony, gdy dane osobowe są przekazywane z państwa członkowskiego do państwa trzeciego lub organizacji międzynarodowej na potrzeby ścigania przestępstw. Jak wskazano powyżej, taka ciągłość ochrony jest ważnym warunkiem szybkiej, skutecznej i pewnej pod względem prawnym współpracy w dziedzinie ścigania przestępstw między zaufanymi partnerami.

---

[144] Wkład EROD w ocenę dyrektywy o ochronie danych w sprawach karnych, pkt 39.
[145] Art. 50 dyrektywy o ochronie danych w sprawach karnych.
[146] Program prac EROD 2021/2022, edpb_workprogramme_2021–2022_en.pdf (europa.eu).

W szczególności, zgodnie z odpowiednimi przepisami dyrektywy o ochronie danych w sprawach karnych[147], międzynarodowe przekazywanie danych między właściwymi organami w rozumieniu dyrektywy o ochronie danych w sprawach karnych musi być oparte na jednym z szeregu narzędzi przekazywania danych określonych w art. 36–38 dyrektywy o ochronie danych w sprawach karnych (jeżeli dane pochodzą z innego państwa członkowskiego, przekazywanie wymaga również uprzedniego zezwolenia tego państwa członkowskiego). Narzędzia te obejmują decyzje stwierdzające odpowiedni stopień ochrony, przekazywanie oparte na odpowiednich zabezpieczeniach oraz stosowanie odstępstw w określonych sytuacjach. Art. 39 dyrektywy o ochronie danych w sprawach karnych dopuszcza również bezpośrednie przekazywanie danych odbiorcom niebędącym organami ścigania, którzy mają siedzibę w państwach trzecich, w indywidualnych i konkretnych przypadkach oraz pod kilkoma warunkami.

3.5.1 Decyzje stwierdzające odpowiedni stopień ochrony

Komisja przyspieszyła swoje prace w celu realizacji pełnego potencjału narzędzi dostępnych w ramach dyrektywy o ochronie danych w sprawach karnych. W czerwcu 2021 r. przyjęła pierwszą „decyzję stwierdzającą odpowiedni stopień ochrony" dotyczącą działań związanych z przetwarzaniem danych na potrzeby ścigania przestępstw, na podstawie art. 36 dyrektywy o ochronie danych w sprawach karnych. Decyzja ta dotyczy Zjednoczonego Królestwa[148]. Decyzja stwierdzająca odpowiedni stopień ochrony umożliwia bezpieczny i swobodny przepływ danych osobowych do właściwych organów danego państwa trzeciego bez potrzeby stosowania dodatkowych zabezpieczeń lub specjalnego zezwolenia (chyba że inne państwo członkowskie, od którego uzyskano dane, musi zezwolić na przekazanie[149]). Decyzja stwierdzająca odpowiedni stopień ochrony danych przez Zjednoczone Królestwo wydana w czerwcu 2021 r. stanowi niezwykle istotny fundament współpracy policyjnej i sądowej po brexicie, która zgodnie z umową o handlu i współpracy między Zjednoczonym Królestwem a UE opiera się na „wieloletnim zobowiązaniu Stron do zapewnienia wysokiego stopnia ochrony danych osobowych"[150]. Zgodnie z art. 36 ust. 4 dyrektywy o ochronie danych w sprawach karnych Komisja monitoruje wszelkie zmiany w ramach prawnych Zjednoczonego Królestwa, które mogłyby mieć wpływ na wspomnianą decyzję stwierdzającą odpowiedni stopień ochrony. Decyzja stwierdzająca odpowiedni stopień ochrony danych przez Zjednoczone Królestwo ma obowiązywać przez okres 4 lat od jej wejścia w życie, zasadniczo z możliwością przedłużenia okresu jej obowiązywania

[147] Zob. art. 35 ust. 3 lit. oraz motyw 64 dyrektywy o ochronie danych w sprawach karnych. Jeżeli chodzi o dalsze przekazywanie danych, zob. art. 35 ust. 1 lit e) oraz motyw 65 dyrektywy o ochronie danych w sprawach karnych.
[148] Decyzja wykonawcza Komisji z 28 czerwca 2021 r. na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo, dostępna na stronie: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32021D1773&qid=1661442538504&from=PL.
[149] Zob. art. 35 ust. 1 lit. c) i art. 35 ust. 2 oraz motyw 66 dyrektywy o ochronie danych w sprawach karnych.
[150] Zob. art. 525 ust. 1 umowy o handlu i współpracy.

o kolejne 4 lata, jeżeli w wyniku monitorowania przez Komisję zostanie potwierdzone, że Zjednoczone Królestwo nadal utrzymuje odpowiedni poziom ochrony[151].

Co więcej, EROD przyczyniła się również do rozwoju tego instrumentu, wydając zalecenie w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy o ochronie danych w sprawach karnych[152], w którym doprecyzowała normę prawną poprzez wskazówki dotyczące elementów, które należy uwzględnić w ocenie odpowiedniego stopnia ochrony danych w kontekście ścigania przestępstw. W szczególności państwo trzecie musi zapewnić prawnie wykonalne prawa indywidualne, skuteczne dochodzenie roszczeń na drodze sądowej oraz niezależny nadzór.

Komisja aktywnie propaguje możliwość ustaleń dotyczących odpowiedniego stopnia ochrony na potrzeby wymiany danych z innymi kluczowymi partnerami międzynarodowymi, w szczególności z tymi państwami, których ścisła i sprawna współpraca jest konieczna w walce z przestępczością i terroryzmem, oraz w z państwami, z którymi już wymienia się znaczne ilości danych osobowych[153]. Do tej pory nie przyjęto wprawdzie żadnych innych decyzji stwierdzających odpowiedni poziom ochrony, jednak wynika to głównie z faktu, że instrument wprowadzono stosunkowo niedawno. Co więcej, i w przeciwieństwie do przetwarzania danych przez podmioty komercyjne, dopiero teraz zaczyna rozwijać się globalna konwergencja zasad ochrony danych w obszarze ścigania przestępstw (napędzana na przykład przez wielostronne ustalenia, takie jak zmieniona konwencja 108 Rady Europy lub drugi protokół dodatkowy do „budapeszteńskiej" Konwencji o cyberprzestępczości). Niemniej jednak doświadczenie zdobyte w wyniku przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony danych przez Zjednoczone Królestwo pomoże utorować drogę dla podobnych inicjatyw w nadchodzących latach. W ramach swojej strategii międzynarodowej Komisja rozważy inne możliwe kandydatury do przyszłych decyzji stwierdzających odpowiedni stopień ochrony na podstawie dyrektywy o ochronie danych w sprawach karnych i uczyni to w bezpośrednim porozumieniu z innymi właściwymi instytucjami i organami UE[154]. W tym celu oraz zgodnie z motywem 68 dyrektywy o ochronie danych w sprawach karnych Komisja zwróci szczególną uwagę na międzynarodowe zobowiązania ocenianych państw dotyczące ochrony danych osobowych, w tym na przystąpienie do wyżej wymienionych porozumień wielostronnych lub do innych instrumentów ochrony porządku publicznego zapewniających odpowiednie zabezpieczenia służące ochronie danych.

---

[151] Zob. pkt 172–174 decyzji stwierdzającej odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo na podstawie dyrektywy o ochronie danych w sprawach karnych, 28 czerwca 2021 r., dostępnej pod adresem: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en

[152] Zalecenia EROD z 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy o ochronie danych w sprawach karnych, przyjęte 2 lutego 2021 r. Zob. również art. 36 ust. 2 oraz motyw 67 dyrektywy o ochronie danych w sprawach karnych.

[153] Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM(2017) 7 final, s. 13–14.

[154] Stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 18.

3.5.2 Odpowiednie zabezpieczenia

Oprócz kompleksowego rozwiązania, jakim jest decyzja stwierdzająca odpowiedni stopień ochrony danych, w dyrektywie o ochronie danych w sprawach karnych przewidziano inne instrumenty przekazywania. Elastyczność tego zestawu narzędzi odzwierciedla art. 37 dyrektywy o ochronie danych w sprawach karnych, który reguluje przekazywanie danych na podstawie „odpowiednich zabezpieczeń" w odniesieniu do ochrony danych osobowych. Takie odpowiednie zabezpieczenia można zapewnić albo za pomocą prawnie wiążącego instrumentu, albo gdy administrator, w oparciu o ocenę wszystkich okoliczności towarzyszących przekazywaniu, dojdzie do wniosku, że istnieją odpowiednie zabezpieczenia („ocena własna" do celów przekazywania).

W pierwszych latach stosowania dyrektywy o ochronie danych w sprawach karnych Komisja pracowała w szczególności nad wiążącymi instrumentami prawnymi w postaci umów międzynarodowych zapewniających odpowiednie zabezpieczenia. Tego rodzaju umowy odgrywają ważną rolę zarówno w kontekście „tradycyjnej" współpracy w dziedzinie ścigania przestępstw (tj. współpracy między właściwymi organami), jak i innych form współpracy (tj. współpracy z udziałem stron trzecich, takich jak przedsiębiorstwa prywatne). Mogą one również służyć jako podstawa przekazywania danych przez Europol i Eurojust w oparciu o odpowiednie ramy prawne, których zasady dotyczące międzynarodowego przekazywania danych są bardzo podobne do zasad obowiązujących w świetle dyrektywy o ochronie danych w sprawach karnych.

Jeżeli chodzi o tradycyjne formy współpracy organów ścigania, Komisja poddaje przeglądowi umowy międzynarodowe przyjęte przez wejściem w życie dyrektywy o ochronie danych w sprawach karnych, aby zapewnić spójność ze zaktualizowanym unijnym systemem ochrony danych[155].

Po pierwsze, Komisja przeprowadza ocenę postanowień dotyczących ochrony danych w obowiązujących umowach o współpracy Europolu[156] z państwami trzecimi zawartych przed 1 maja 2017 r., zgodnie z rozporządzeniem (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (zwanym dalej „rozporządzeniem w sprawie Europolu")[157].

---

[155] W swoim komunikacie w sprawie dalszych działań mających na celu dostosowanie dorobku prawnego należącego do dawnego trzeciego filaru do przepisów dotyczących ochrony danych Komisja stwierdziła, że szereg obowiązujących umów nie wymaga dalszego dostosowania do dyrektywy o ochronie danych w sprawach karnych (np. porozumienie między Unią Europejską a Republiką Islandii oraz Królestwem Norwegii w sprawie stosowania niektórych postanowień Konwencji z dnia 29 maja 2000 roku o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej oraz Protokołu z 2001 roku do Konwencji).

[156] Więcej informacji na temat obowiązujących umów Europolu można znaleźć na stronie internetowej tej agencji pod adresem: https://www.europol.europa.eu/partners-collaboration/agreements.

[157] Zob. art. 25 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępującego i uchylającego 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.

Zgodnie z art. 9 protokołu nr 36 do Traktatu o Unii Europejskiej[158] oraz TFUE (w sprawie postanowień przejściowych) skutki prawne tych umów zostają utrzymane do czasu ich uchylenia, unieważnienia lub zmiany[159]. Komisja poinformuje Parlament Europejski i Radę o wyniku tej oceny oraz, w stosownych przypadkach, przedłoży Radzie zalecenie dotyczące decyzji upoważniającej do rozpoczęcia negocjacji w celu zmiany odpowiedniej umowy lub umów zgodnie z art. 218 TFUE. Jest to złożone zadanie, które obejmuje ocenę 18 umów i którego wykonanie opóźniło się przez zakłócenia spowodowane pandemią COVID-19. Komisja zamierza zakończyć proces oceny w drugiej połowie 2022 r.

Spójność wszystkich mechanizmów współpracy organów ścigania z przepisami dyrektywy o ochronie danych w sprawach karnych stanowi zasadę przewodnią, którą Komisja kieruje się również podczas negocjowania nowych umów dotyczących przekazywania danych osobowych przez Europol państwom trzecim lub organizacjom międzynarodowym. Od wejścia w życie w 2017 r. obecnego rozporządzenia w sprawie Europolu podstawę prawną takich umów międzynarodowych, zapewniającą odpowiednie zabezpieczenia, stanowi art. 218 TFUE. W latach 2018 i 2019 Rada przyjęła dziewięć mandatów upoważniających Komisję do rozpoczęcia negocjacji z państwami trzecimi w imieniu Unii. Komisja została również upoważniona do rozpoczęcia negocjacji w sprawie umowy o współpracy z Interpolem, która obejmowałaby wymianę danych z kilkoma organami i agencjami UE. We wszystkich powyższych przypadkach Rada skierowała do Komisji wytyczne negocjacyjne, aby zapewnić uwzględnienie niezbędnych zabezpieczeń w zakresie ochrony danych osobowych oraz innych podstawowych praw i wolności osób fizycznych. Na tej podstawie Komisja zakończyła już negocjacje z Nową Zelandią, w wyniku których 30 czerwca 2022 r. podpisano umowę o współpracy. Osiągnięto także postęp w negocjacjach z Izraelem. Negocjacje z Turcją są na zaawansowanym etapie, ale nie mogą zostać zakończone, dopóki Turcja nie przeprowadzi niezbędnych reform swojego prawodawstwa w zakresie ochrony danych. W marcu 2021 r. Komisja otrzymała podobne upoważnienia do negocjowania umów o współpracy, które umożliwiałyby Eurojustowi wymianę danych z 13 państwami trzecimi.

Po drugie, Komisja przeprowadza obecnie pierwszy wspólny przegląd umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych (zwanej dalej „umową ramową"). Umowa ramowa, która weszła w życie w lutym 2017 r., zawiera kompleksowy i zharmonizowany zestaw przepisów o ochronie danych, które stosuje się do wszystkich transatlantyckich wymian między właściwymi organami. Stanowi ona uzupełnienie istniejących umów zawartych między organami ścigania UE i USA oraz między organami ścigania państw członkowskich UE i USA, ustanawia normy wysokiego poziomu ochrony na potrzeby przyszłych umów w tej dziedzinie oraz wzmacnia

[158] Wersja skonsolidowana Traktatu Unii Europejskiej, Dz.U. C 202 z 7.6.2016, dostępna na stronie: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:02016M/TXT-20200301.
[159] Motyw 35 rozporządzenia w sprawie Europolu.

współpracę organów ścigania poprzez ułatwienie wymiany informacji. Celem wspomnianego wspólnego przeglądu jest ocena skuteczności wdrażania umowy ramowej, w szczególności w odniesieniu do przepisów dotyczących dalszego przekazywania, praw indywidualnych oraz sądowych środków zaskarżenia. Harmonogram wspólnego przeglądu zmienił się w wyniku zakłóceń związanych z pandemią COVID-19, a także toczących się równolegle negocjacji w sprawie drugiego protokołu dodatkowego do „budapeszteńskiej" Konwencji Rady Europy o cyberprzestępczości[160].Komisja zamierza zakończyć wspólny przegląd w drugiej połowie 2022 r.

Umowa ramowa, jako pierwsza dwustronna umowa międzynarodowa zawierająca kompleksowy katalog praw i obowiązków w zakresie ochrony danych, stanowi punkt odniesienia podczas negocjacji mających na celu zawarcie podobnych umów ramowych z ważnymi partnerami w zakresie ścigania przestępstw[161]. W trakcie takich negocjacji Komisja uwzględni również istotne zmiany, w tym wytyczne EROD, orzecznictwo TSUE oraz wynik międzynarodowych negocjacji w sprawie zabezpieczeń w zakresie ochrony danych w tym obszarze (takich jak np. drugi protokół dodatkowy do Konwencji o cyberprzestępczości lub umowa Europolu z Nową Zelandią[162]).

Po trzecie, Komisja uznała umowę między Unią Europejską a Japonią w sprawie wzajemnej pomocy prawnej w sprawach karnych („traktat o pomocy prawnej UE–Japonia")[163] za akt prawny UE regulujący przetwarzanie (przekazywanie) danych na potrzeby ścigania przestępstw, który należy zmienić w celu zapewnienia odpowiednich zabezpieczeń w zakresie ochrony danych zgodnie z dyrektywą o ochronie danych w sprawach karnych. Po wydaniu przez Radę decyzji[164] upoważniającej do podjęcia negocjacji w celu zmiany traktatu o pomocy prawnej UE–Japonia Komisja prowadzi dalsze rozmowy z władzami japońskimi, zmierzające do jak najszybszego rozpoczęcia negocjacji.

Co więcej, obecnie w coraz większym stopniu stosuje się również inne formy współpracy dostosowane do szczególnych wyzwań i potrzeb związanych z postępowaniami przygotowawczymi w dzisiejszej gospodarce cyfrowej. Formy te dotyczą głównie wzmocnionej współpracy w dziedzinie cyberprzestępczości i do celów zbierania elektronicznych materiałów

---

[160]Komisja, w imieniu Unii Europejskiej, oraz Stany Zjednoczone były mocno zaangażowane w te negocjacje, w tym w ramach specjalnej podgrupy ds. ochrony danych (ochrona danych była jednym z najszerzej omawianych tematów).

[161] Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM(2017) 7 final, s. 14.

[162] Umowa między Unią Europejską, z jednej strony, a Nową Zelandią, z drugiej strony, dotycząca wymiany danych osobowych między Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) i właściwymi organami ds. zwalczania poważnej przestępczości i terroryzmu w Nowej Zelandii.

[163] Umowa w sprawie wzajemnej pomocy prawnej w sprawach karnych między Unią Europejską a Japonią, Dz.U. L 39 z 12.2.2010, s. 20.https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A22010A0212%2801%29.

[164] Decyzja Rady upoważniająca do podjęcia negocjacji z Japonią w sprawie zmiany umowy między Unią Europejską a Japonią w sprawie wzajemnej pomocy prawnej w sprawach karnych (dokument LT 223/21).

dowodowych dotyczących przestępstw. Współpraca ta obejmuje bezpośrednią współpracę z podmiotami prywatnymi w zakresie dostępu do elektronicznych materiałów dowodowych.

Komisja nawiązała również współpracę z partnerami międzynarodowymi w celu zapewnienia, aby te inne (ważne) formy współpracy mogły być realizowane przy zachowaniu zabezpieczeń w zakresie ochrony danych osobowych.

Po pierwsze, Komisja reprezentowała Unię Europejską podczas negocjacji[165] w ramach Rady Europy w sprawie drugiego protokołu dodatkowego do „budapeszteńskiej" Konwencji o cyberprzestępczości[166]. Protokół ten, który został zatwierdzony przez Komitet Ministrów Rady Europy 17 listopada 2021 r., zawiera solidne zabezpieczenia w zakresie ochrony praw podstawowych, w tym artykuł[167] zawierający szczegółowe przepisy dotyczące ochrony danych osobowych przekazywanych na podstawie protokołu. Przepisy te obejmują wszystkie podstawowe zasady ochrony danych, prawa i obowiązki uznawane w prawie Unii. Gwarancje te uzupełnia przepis dotyczący monitorowania oraz możliwość zawieszenia przekazywania danych osobowych w przypadku systematycznego lub istotnego naruszenia zabezpieczeń określonych w protokole, na przykład w przypadku braku skutecznych środków odwoławczych na drodze sądowej. Dzięki tym przepisom Komisja zapewnia odpowiednie zabezpieczenia zgodnie z wymogami określonymi w art. 37 ust. 1 lit. a) dyrektywy o ochronie danych w sprawach karnych[168]. Jest to znaczące osiągnięcie, biorąc pod uwagę zróżnicowane członkostwo w Konwencji o cyberprzestępczości, której stronami jest obecnie 66 państw, reprezentujących różne systemy i tradycje prawne. Dzięki temu właściwe organy państw członkowskich będą mogły czerpać korzyści ze skutecznej współpracy transgranicznej w walce z cyberprzestępczością, przy jednoczesnym zapewnieniu poszanowania wartości UE odzwierciedlonych w Karcie praw podstawowych Unii Europejskiej, traktatach UE i prawie wtórnym UE. Biorąc pod uwagę dużą liczbę stron Konwencji o cyberprzestępczości, która obejmuje obecnie kraje z całego świata, protokół pomoże również promować wysokie standardy ochrony danych w zakresie przetwarzania danych w obszarze ścigania przestępstw na szczeblu globalnym. Protokół został otwarty do podpisu 12 maja 2022 r.,

---

[165] Po zatwierdzeniu mandatu przez Radę Unii Europejskiej 6 czerwca 2019 r. Mandat ten jest dostępny na stronie: https://www.consilium.europa.eu/pl/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[166] Drugi protokół dodatkowy do Konwencji o cyberprzestępczości w sprawie wzmocnionej współpracy i ujawniania elektronicznego materiału dowodowego został zatwierdzony przez Komitet Ministrów Rady Europy 17 listopada 2021 r. Protokół ten został sporządzony przez komitet Konwencji o cyberprzestępczości (T-CY) w okresie od września 2017 r. do maja 2021 r. Tekst protokołu (uwierzytelniony odpis) jest dostępny na stronie https://rm.coe.int/1680a4b2e1. Sprawozdanie wyjaśniające do protokołu jest również dostępne na stronie https://rm.coe.int/1680a49c9d

[167] Zob. art. 14 protokołu dodatkowego wraz z pkt 220–287 sprawozdania wyjaśniającego.

[168] W opinii nr 1/2022 z 20 stycznia 2022 r. w sprawie projektu decyzji Rady upoważniających do podpisania i ratyfikacji protokołu dodatkowego EIOD „z aprobatą przyjmuje liczne zabezpieczenia, które zostały włączone do protokołu".

a podpisały go już łącznie 22 strony Konwencji o cyberprzestępczości (w tym 13 państw członkowskich UE).

Po drugie, Komisja rozpoczęła negocjacje w sprawie umowy dwustronnej ze Stanami Zjednoczonymi w sprawie transgranicznego dostępu do dowodów elektronicznych na potrzeby współpracy wymiarów sprawiedliwości w sprawach karnych[169]. Umowa ta ma na celu uwzględnienie elektronicznego materiału dowodowego w postaci zarówno danych nieosobowych, jak i danych osobowych, w tym danych o ruchu i danych dotyczących treści. Co ważne, negocjacje mają również na celu włączenie do tej umowy dodatkowych zabezpieczeń w zakresie ochrony danych, które uzupełniałyby te zawarte w umowie ramowej, biorąc pod uwagę w szczególności wrażliwość poszczególnych kategorii przedmiotowych danych, a także wymagania dotyczące przekazywania elektronicznych materiałów dowodowych bezpośrednio przez dostawców usług. Postępy w tych negocjacjach będą w dużej mierze zależeć od postępów w trwającym procesie legislacyjnym dotyczącym unijnego elektronicznego materiału dowodowego[170].

Te różne inicjatywy Komisji mające na celu opracowanie międzynarodowych instrumentów ułatwiających współpracę organów ścigania z partnerami międzynarodowymi przy jednoczesnym zapewnieniu odpowiednich zabezpieczeń służących ochronie danych były wspierane działaniami EROD i EIOD. Działania te obejmowały oświadczenie EROD w sprawie nowego projektu przepisów drugiego protokołu dodatkowego do Konwencji o cyberprzestępczości[171] oraz opinie EIOD w sprawie projektów mandatów negocjacyjnych dotyczących umów międzynarodowych na podstawie art. 218 TFUE, które umożliwiłyby Europolowi i Eurojustowi wymianę danych osobowych z państwami trzecimi lub organizacjami międzynarodowymi[172]. EROD wydała również oświadczenie, w którym zachęca państwa członkowskie do oceny i, w razie potrzeby, przeglądu umów międzynarodowych obejmujących międzynarodowe przekazywanie danych

---

[169] Decyzja Rady upoważniająca do rozpoczęcia negocjacji w celu zawarcia porozumienia między Unią Europejską a Stanami Zjednoczonymi Ameryki w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego na potrzeby współpracy wymiarów sprawiedliwości w sprawach karnych. Mandat ten jest dostępny na stronie: https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/pl/pdf.

[170] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych, (COM(2018) 225 final), oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych, (COM(2018) 226 final).

[171] EROD, Oświadczenie nr 02/2021 w sprawie nowego projektu przepisów drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (Konwencja o cyberprzestępczości), przyjęte 2 lutego 2021 r., dostępne na stronie internetowej https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_pl

[172] EIOD, opinia nr 04/2021 w sprawie przeglądu mandatu Europolu, przyjęta 8 marca 2021 r., dostępna na stronie https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-europol-regulation_en.

osobowych[173]. Oświadczenie to dotyczy umów, które zostały zawarte przed 6 maja 2016 r., między innymi w obszarze ścigania przestępstw, i zachęca się w nim państwa członkowskie do ustalenia, czy wymagane jest dalsze dostosowanie do przepisów i orzecznictwa UE o ochronie danych.

W art. 37 dyrektywy o ochronie danych w sprawach karnych zezwala się również na międzynarodowe przekazywanie danych w oparciu o własną ocenę dokonaną przez właściwy organ, czy państwo trzecie (lub organizacja międzynarodowa) posiada odpowiednie zabezpieczenia służące ochronie danych. W tych przypadkach organ musi udokumentować przekazanie (w tym jego datę i godzinę, informacje o organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe), a dokumentacja musi być udostępniona na żądanie organowi nadzorczemu (art. 37 ust. 3 dyrektywy o ochronie danych w sprawach karnych). Informacje zwrotne przekazane przez państwa członkowskie[174] wskazują, że narzędzie to było rzadko stosowane.

Aby umożliwić państwom członkowskim pełne wykorzystanie zestawu narzędzi związanych z przekazywaniem danych, który przewidziano w dyrektywie o ochronie danych w sprawach karnych, EROD powinna zintensyfikować swoje bieżące prace nad poszczególnymi mechanizmami przekazywania. Powinna między innymi przedstawiać wytyczne dotyczące mechanizmów określonych w art. 37 ust. 1 dyrektywy o ochronie danych w sprawach karnych, a zwłaszcza przekazywania danych w oparciu o ocenę własną dokonywaną przez właściwe organy. Tę potrzebę podkreśliła również Rada[175].

3.5.3 Stosowanie wyjątków

Na koniec należy stwierdzić, że tak zwane „wyjątki" zapewniają ważną podstawę do przekazywania pod pewnymi warunkami, określonymi w art. 38 dyrektywy o ochronie danych w sprawach karnych. Warunki te zapewniają równowagę między względami prywatności a potrzebami operacyjnymi właściwych organów. W szczególności art. 38 ust. 1 zezwala na przekazanie, a nawet na określone kategorie przekazywania danych osobowych, gdy jest to niezbędne do zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa

[173] EROD, oświadczenie nr 04/2021 w sprawie umów międzynarodowych, w tym przekazywania danych osobowych, przyjęte 13 kwietnia 2021 r. Dostępne pod adresem https://edpb.europa.eu/system/files/2021-04/edpb_statement042021_international_agreements_including_transfers_en.pdf

[174] Zob. sprawozdanie prezydencji Rady Unii Europejskiej w sprawie wymiany danych policyjnych z państwami trzecimi – doświadczenia w stosowaniu art. 37 dyrektywy o ochronie danych w sprawach karnych. EROD ogłosiła, że uwzględni wnioski ze sprawozdania prezydencji wraz z dalszymi informacjami i uwagami państw członkowskich w swoich działaniach na rzecz opracowania wytycznych dotyczących art. 37 dyrektywy. Zob. pismo przewodniczącej EROD do stałego przedstawicielstwa Republiki Federalnej Niemiec przy Unii Europejskiej z 26 lutego 2021 r. (dokument 13555/1/20).

[175] Zob. stanowisko i ustalenia Rady w sprawie stosowania dyrektywy o ochronie danych w sprawach karnych, pkt 20.

publicznego[176] lub, w indywidualnych przypadkach, do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych[177]. W przeciwieństwie do wyjątków stosowanych na podstawie art. 49 RODO nie istnieją obecnie żadne wytyczne dotyczące stosowania wyjątków na podstawie art. 38 dyrektywy o ochronie danych w sprawach karnych.

3.5.4 Skuteczna współpraca policyjna i sądowa ponad granicami

Dyrektywa o ochronie danych w sprawach karnych stała się już międzynarodowym punktem odniesienia w kontekście ścigania przestępstw i stanowiła katalizator dla krajów na całym świecie, aby rozważyć wprowadzenie nowoczesnych przepisów dotyczących prywatności w tym obszarze. Jest to bardzo pozytywna zmiana, która stwarza nowe możliwości lepszej ochrony osób fizycznych w UE w przypadku, gdy ich dane są przekazywane za granicę do celów ścigania przestępstw, a jednocześnie ułatwia przepływ danych, które mogą pomóc w zwalczaniu przestępczości.

Bardziej ogólnie rzecz ujmując, trzeba zagwarantować, aby w przypadku otrzymania bezpośredniego wniosku o współpracę w zakresie udostępnienia danych do celów ścigania przestępstw przedsiębiorstwo działające na rynku europejskim mogło takie dane udostępnić bez ryzyka kolizji przepisów i przy pełnym poszanowaniu praw podstawowych UE[178]. Aby usprawnić takie przekazywanie danych, Komisja zobowiązuje się do opracowania odpowiednich ram prawnych wspólnie z partnerami międzynarodowymi w celu unikania kolizji przepisów i wspierania efektywnych form współpracy, zwłaszcza przez zapewnienie niezbędnych zabezpieczeń w zakresie ochrony danych, a tym samym przyczynienia się do skuteczniejszej walki z przestępczością.

W tym kontekście Komisja podjęła działania a forach dwustronnych, regionalnych i wielostronnych w celu aktywnego propagowania międzynarodowej konwergencji norm ochrony danych na potrzeby współpracy organów ścigania. W dialogu Komisji z kilkoma zagranicznymi krajami partnerskimi w sprawie trwających u nich reform ustaw o ochronie danych służby Komisji uczestniczyły w różny sposób (np. składając uwagi w odpowiedzi na konsultacje publiczne, uczestnicząc w przesłuchaniach parlamentarnych oraz specjalnych spotkaniach z przedstawicielami rządu i decydentami) w opracowanie przepisów dotyczących przetwarzania danych osobowych przez właściwe organy.

Na szczeblu regionalnym i wielostronnym Komisja wspiera na przykład projekty budowania zdolności w kontekście wdrażania Konwencji o cyberprzestępczości Rady Europy[179]. Projekty te obejmują program GLACY+, mający na celu wzmocnienie zdolności państw do stosowania

---

[176] Art. 38 ust. 1 lit. c) dyrektywy o ochronie danych w sprawach karnych.
[177] Art. 38 ust. 1 lit d) dyrektywy o ochronie danych w sprawach karnych.
[178] Na przykład drugi protokół dodatkowy do Konwencji o cyberprzestępczości można uznać za umowę międzynarodową do celów art. 48 RODO.
[179] Zob. https://www.coe.int/en/web/cybercrime/glacyplus.

przepisów dotyczących cyberprzestępczości oraz zwiększenie ich zdolności do skutecznej współpracy międzynarodowej zgodnie z Konwencją o cyberprzestępczości i jej protokołami dodatkowymi. Wiąże się to również z opracowaniem przepisów dotyczących ochrony danych obejmujących przetwarzanie danych na tym obszarze. Program wspiera obecnie 17 krajów priorytetowych i węzłowych w Afryce, regionie Azji i Pacyfiku, Ameryce Łacińskiej i regionie Karaibów.

Komisja nawiązała również współpracę z Ameripolem, organizacją współpracy policyjnej skupiającą 18 państw Ameryki Łacińskiej, w celu opracowania ram ochrony danych na potrzeby wymiany informacji między Ameripolem a jego państwami członkowskimi. Współpraca ta odbywa się w ramach projektu EL PAcCTO: Support to Ameripol [Wsparcie dla Ameripolu], którego celem jest podniesienie poziomu współpracy międzynarodowej między organami policyjnymi, sądowymi i prokuratorskimi krajów partnerskich w zakresie zwalczania przestępczości zorganizowanej.

Komisja propaguje również zmienioną konwencję nr 108 (znaną jako konwencja nr 108+)[180], która ma zastosowanie także do działań związanych z przetwarzaniem danych na potrzeby ścigania przestępstw. Konwencja ta, do której mogą przystępować również państwa niebędące członkami Rady Europy, jest ważna nie tylko dlatego, że jest jedyną wielostronną wiążącą umową dotyczącą ochrony danych, ale również dlatego, że Komitet Konwencji zapewnia forum wymiany najlepszych praktyk i ustanawiania światowych standardów[181]. W ramach swojej międzynarodowej strategii dotyczącej przepływu danych Komisja zachęca państwa trzecie do przystąpienia do konwencji nr 108+.

Komisja zachęca ponadto do zwiększania konwergencji na poziomie międzynarodowym poprzez dzielenie się z partnerami naszym doświadczeniem w zakresie aspektów ochrony danych w ramach współpracy organów ścigania. Powołana przez Komisję „Akademia Ochrony Danych", będąca częścią projektu „Międzynarodowa współpraca cyfrowa – wzmocniona ochrona danych i przepływ danych" finansowanego w ramach Instrumentu Polityki Zagranicznej, jest kluczowym narzędziem służącym do realizacji tego przedsięwzięcia. Akademię utworzono w celu wspierania wymian między organami regulacyjnymi w Europie i w państwach trzecich i usprawnienia współpracy w terenie. Jej działalność obejmuje wszystkie aspekty nadzoru nad ochroną danych, w tym w dziedzinie ścigania przestępstw.

---

[180] Protokół zmieniający do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przyjęty przez Komitet Ministrów Rady Europy na 128. posiedzeniu w Elsinore w dniu 18 maja 2018 roku (konwencja nr 108+), dostępny na stronie https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[181] Zob. na przykład „Praktyczny przewodnik dotyczący wykorzystywania danych osobowych w sektorze policji", dostępny na stronie https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

4 DALSZE DZIAŁANIA

Aby zapewnić skuteczną politykę bezpieczeństwa UE, w pełni zgodną z prawem podstawowym do ochrony danych osobowych, Komisja będzie nadal kontrolować prawidłową transpozycję przez państwa członkowskie dyrektywy o ochronie danych w sprawach karnych i monitorować stosowanie jej przepisów.

Dyrektywa o ochronie danych w sprawach karnych w znacznym stopniu przyczyniła się do bardziej zharmonizowanego i wyższego poziomu ochrony praw osób fizycznych oraz do bardziej spójnych ram prawnych dla właściwych organów.

Dyrektywa została zasadniczo transponowana w sposób zadowalający, lecz wskazano na szereg problemów. Komisja wszczęła już postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego dotyczące zarówno braku transpozycji dyrektywy o ochronie danych w sprawach karnych, jak i niezgodności prawa krajowego z jej przepisami. Komisja będzie kontynuować prace na rzecz zapewnienia pełnej i prawidłowej transpozycji tej dyrektywy.

Dyrektywa o ochronie danych w sprawach karnych doprowadziła do zwiększenia poziomu świadomości właściwych organów krajowych dotyczącej ochrony danych oraz uwagi poświęcanej tej kwestii, również w odniesieniu do bezpieczeństwa przetwarzania.

Aktywny nadzór ze strony organów nadzorujących ochronę danych ma zasadnicze znaczenie dla zapewnienia wypełnienia w praktyce celów dyrektywy o ochronie danych w sprawach karnych. Organom tym należy zatem przyznać wszystkie rodzaje uprawnień wymaganych na podstawie dyrektywy o ochronie danych w sprawach karnych, wraz z odpowiednimi zasobami.

Na tym etapie należy skupić się na wykorzystaniu pełnego potencjału dyrektywy o ochronie danych w sprawach karnych. W tym kontekście i biorąc pod uwagę ograniczone doświadczenie w stosowaniu tych nowych przepisów, Komisja uważa, że jest zbyt wcześnie, aby rozważać zmianę dyrektywy o ochronie danych w sprawach karnych.

Komisja będzie nadal aktywnie współpracować ze wszystkimi zainteresowanymi stronami w perspektywie kolejnej oceny, która ma zostać przeprowadzona do 2026 r. W międzyczasie będzie kontynuować prace nad zapewnieniem spójności z innymi przepisami UE, które są istotne dla przetwarzania danych osobowych na potrzeby ścigania przestępstw.

Ramy prawne

Komisja zamierza:

- kontynuować ocenianie transpozycji dyrektywy o ochronie danych w sprawach karnych przez państwa członkowskie i w razie potrzeby podejmować odpowiednie działania (w tym wszczynać postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego);
- nadal prowadzić wymianę dwustronną z państwami członkowskimi;
- zapewniać, aby przyszłe wnioski ustawodawcze były zgodne z dyrektywą o ochronie danych w sprawach karnych.

Państwa członkowskie powinny:

- zapewnić pełną i prawidłową transpozycję dyrektywy o ochronie danych w sprawach karnych na szczeblu krajowym, między innymi określając niezbędne wymogi wynikające z dyrektywy o ochronie danych w sprawach karnych, jeżeli nie są one określone w krajowych aktach o ochronie danych transponujących tę dyrektywę.

Nadzór sprawowany przez organy nadzorujące ochronę danych

Państwa członkowskie powinny:

- zapewnić organom nadzorującym ochronę danych wystarczające zasoby do wykonywania zadań związanych z egzekwowaniem przepisów dyrektywy o ochronie danych w sprawach karnych;
- zapewnić, aby organy nadzorujące ochronę danych mogły wykonywać wszystkie rodzaje uprawnień określonych w dyrektywie o ochronie danych w sprawach karnych;
- systematycznie zasięgać opinii swoich organów nadzorujących ochronę danych w sprawie projektów przepisów i środków administracyjnych o zastosowaniu ogólnym, dotyczących ochrony danych osobowych, oraz należycie uwzględniać ich opinie (zwłaszcza w przypadku nowych technologii).

Organy nadzorujące ochronę danych wzywa się do:

- pełnego wykorzystywania swoich uprawnień w zakresie prowadzenia postępowań, w tym poprzez przeprowadzanie inspekcji z własnej inicjatywy;
- gromadzenia określonych danych statystycznych dotyczących działań nadzorczych prowadzonych przez nie na podstawie dyrektywy o ochronie danych w sprawach karnych;
- wykorzystywania narzędzi wzajemnej pomocy i opracowania praktycznych środków ułatwiających składanie wniosków o pomoc, w tym poprzez planowane wytyczne EROD.

EROD wzywa się do:

- rozszerzenia puli ekspertów wspierających[182] do zadań związanych z dyrektywą o ochronie danych w sprawach karnych.

Udzielanie wsparcia właściwym organom

Komisja zamierza:

- umożliwiać prowadzenie dyskusji oraz wymianę doświadczeń między państwami członkowskimi oraz Komisją w ramach reprezentującej państwa członkowskie grupy ekspertów ds. dyrektywy o ochronie danych w sprawach karnych;
- umożliwiać wymianę poglądów między inspektorami ochrony danych za pośrednictwem sieci inspektorów ochrony danych.

Państwa członkowskie wzywa się do:

[182] Dokument EROD w sprawie mandatu puli ekspertów wspierających EROD przyjęty 15 grudnia 2020 r.

- kontynuowania działań na potrzeby zapewnienia właściwym organom szkoleń na temat wymogów ochrony danych, w tym w odniesieniu do nowych technologii.

EROD oraz organy nadzorujące ochronę danych wzywa się do:

- wzmocnienia działań na rzecz przyjęcia odpowiednich wytycznych (np. dotyczących roli zgody w kontekście przetwarzania danych osobowych do celów ścigania przestępstw oraz praw osób, których dane dotyczą, w tym ich ewentualnych ograniczeń) poprzez przyjęcie nowych samodzielnych wytycznych albo uzupełnienie wytycznych już przyjętych na potrzeby RODO.

Transgraniczne przekazywanie danych

Komisja zamierza:

- aktywnie propagować wśród kluczowych partnerów międzynarodowych ewentualne nowe decyzje stwierdzające odpowiedni stopień ochrony;
- negocjować nowe umowy o współpracy między Europolem i Eurojustem z jednej strony, a państwami trzecimi z drugiej. W razie potrzeby Komisja będzie dążyć do renegocjacji istniejących umów o współpracy z Europolem w celu uwzględnienia w nich odpowiednich zabezpieczeń służących ochronie danych;
- podjąć negocjacje z Japonią w celu zmiany istniejącej umowy w sprawie wzajemnej pomocy prawnej między UE a Japonią, aby zapewnić odpowiednie zabezpieczenia służące ochronie danych;
- kontynuować i zakończyć negocjacje w sprawie umowy dwustronnej ze Stanami Zjednoczonymi w sprawie transgranicznego dostępu do elektronicznego materiału dowodowego na potrzeby współpracy wymiarów sprawiedliwości w sprawach karnych, między innymi uzupełniając zabezpieczenia służące ochronie danych zagwarantowane w umowie ramowej między UE a USA, aby odzwierciedlić specyficzny kontekst bezpośredniej współpracy organów ścigania z dostawcami usług;
- zbadać możliwość zawarcia z ważnymi partnerami będącymi organami ścigania umów ramowych o przetwarzaniu danych w obszarze ścigania przestępstw, opierając się na przykładzie umowy ramowej między UE a USA.

EROD wzywa się do:

- przyjęcia wytycznych w celu doprecyzowania pojęcia i treści „odpowiednich zabezpieczeń" (art. 37 dyrektywy o ochronie danych w sprawach karnych), jak również zasad stosowania wyjątków (art. 38 dyrektywy o ochronie danych w sprawach karnych).

Promowanie konwergencji i rozwijanie współpracy międzynarodowej

Komisja zamierza:

- rozszerzyć współpracę z partnerami międzynarodowymi w celu wzmocnienia konwergencji przepisów o ochronie danych w dziedzinie ścigania przestępstw, między innymi poprzez

propagowanie przystąpienia do konwencji nr 108+ jako jedynej wiążącej ogólnoświatowej umowy o ochronie danych;

- propagować współpracę dwustronną, regionalną i wielostronną oraz wspierać projekty budowania zdolności w dziedzinie ochrony danych i współpracy policyjnej. Będzie to obejmować szkolenia oraz wymianę wiedzy i najlepszych praktyk za pośrednictwem Akademii Ochrony Danych.

Państwa członkowskie wzywa się do:

- szybkiego ratyfikowania drugiego protokołu dodatkowego do „budapeszteńskiej" Konwencji Rady Europy o cyberprzestępczości, gdy tylko zostaną do tego upoważnione decyzją Rady.