ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3744
PRZEGLĄD PRAWA I ADMINISTRACJI CVII
WROCŁAW 2016
DOI: 10.19195/0137-1134.107.3

PATRYCJA DĄBROWSKA-KŁOSIŃSKA
Centrum Europejskie UW

STOSOWANIE UNIJNYCH PRZEPISÓW O TRANSGRANICZNYCH ZAGROŻENIACH DLA ZDROWIA A OCHRONA DANYCH OSOBOWYCH W UE

1. WPROWADZENIE

Zgodnie z art. 168 Traktatu o Funkcjonowaniu Unii Europejskiej polityka UE w dziedzinie ochrony zdrowia publicznego uzupełnia polityki państw członkowskich i ma na celu polepszanie zdrowia, zapobieganie chorobom i usuwanie źródeł zagrożeń dla zdrowia[1]. Działanie Unii obejmuje więc także zwalczanie epidemii i polega, w szczególności, na wspieraniu badań naukowych, wymianie informacji zdrowotnej, a także na monitorowaniu poważnych transgranicznych zagrożeń zdrowia, wczesnym ostrzeganiu oraz ich zwalczaniu. Te ostatnie kwestie są uregulowane szczegółowo w prawie wtórnym — przede wszystkim — w decyzji 1082/2013 w sprawie poważnych transgranicznych zagrożeń zdrowia (dalej „decyzja 1082/2013"). Właściwymi unijnymi organami są Komisja Europejska (Dyrekcja Generalna ds. Zdrowia, *DG SANTE*) i Europejskie Centrum ds. Zapobiegania i Kontroli Chorób („ECDC") ustanowione rozporządzeniem 851/2004[2].

W konsekwencji w UE istnieją szczegółowe przepisy prawne i uprawnione instytucje, których celem jest zapobieganie i zwalczanie transgranicznych zagrożeń dla zdrowia ludzkiego, takich jak epidemiczne choroby zakaźne czy zagrożenia o pochodzeniu chemicznym, w tym terrorystyczne[3]. Ta regulacja przeciwdziałania zagrożeniom na poziomie unijnym odbywa się na przykład przez możli-

[1] Por. Komentarz do artykułu 168 [w:] *Komentarz do Traktatu o Funkcjonowaniu Unii Europejskiej*, t. 2, red. K. Kowalik-Bańczyk, M. Szwarc, A. Wróbel, Warszawa 2012. Zob. też ogólnie T.K. Hervey, J. McHale, *European Union Health Law: Themes and Implications*, Cambridge 2015.

[2] Por. punkty 1–10 preambuły do decyzji nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE, Dz. Urz. UE 2013, L 293/1; oraz rozporządzenie (WE) nr 851/2004 z dnia 21 kwietnia 2004 r. ustanawiające Europejskie Centrum ds. Zapobiegania i Kontroli Chorób, Dz. Urz. UE 2004, L 142/1.

[3] Por. w tym kontekście D.L. Heymann, *The Evolving Infectious Disease Threat: Implications for National and Global Security*, „Journal of Human Development" 4 (2), 2003, s. 191–207.

wość zorganizowania wspólnych zamówień na medyczne środki zapobiegawcze, a przede wszystkim za pośrednictwem wymiany informacji między instytucjami UE i uprawnionymi władzami państw członkowskich przez sieć nadzoru i kontroli epidemiologicznej, monitorowanie i wczesne ostrzeganie (tzw. Europejski System Wczesnego Ostrzegania i Reagowania — „EWRS"), ponieważ UE działa w ramach traktatowej kompetencji[4]. W efekcie regulacji decyzji 1082/2013 państwa członkowskie i Komisja są zobowiązane do pełnej koordynacji reagowania na poważne transgraniczne zagrożenia zdrowia na szczeblu krajowym i unijnym, pełnej komunikacji wzajemnej w zakresie ryzyka, sytuacji kryzysowych i zastosowanych środków ochrony zdrowia oraz konsultacji w ramach Komitetu ds. Bezpieczeństwa Zdrowia („KBZ").

Właśnie te przepisy i instrumenty unijne służące bezpieczeństwu zdrowia, które opierają się na wymianie informacji epidemiologicznych i medycznych, w tym potencjalnie danych osobowych jednostek, będą przedmiotem analizy w niniejszym artykule. Potencjalny konflikt dóbr ochrony zdrowia publicznego i danych osobowych jednostek wpisuje się zresztą w znacznie szerszą problematykę wyważania sprzeczności chronionych wartości i konieczności godzenia interesów: bezpieczeństwa publicznego i praw podstawowych[5]. Natomiast system zarządzania wielopoziomowego zagrożeniami dla zdrowia publicznego (*multi--level governance*) wynika z oczywistej niemożliwości przeciwdziałania takim zagrożeniom jak szybko rozprzestrzeniające się choroby zakaźne przez pojedyncze państwa członkowskie UE wobec obecnego rozwoju międzynarodowego przepływu osób[6]. System unijny jest też wynikiem wprowadzenia rozwiązań na poziomie globalnym, gdzie kwestie zapewniania bezpieczeństwa sanitarnego są uregulowane przez Międzynarodowe Przepisy Zdrowotne wydane w ramach Światowej Organizacji Zdrowia[7].

Tekst omawia i analizuje kolejno: prawo do ochrony danych osobowych w UE (część 2); studium przypadku międzynarodowego turysty poszukiwanego

[4] Art. 5–8 oraz 11, 15 i 17–18, decyzja 1082/2013. Zob. też G. Majone, *The New European Agencies: Regulation by Information*, „Journal of European Public Policy" 4 (2), 1997.

[5] Zob. np. B.J. Gold, L. Lazarus, *Security and Human Rights*, Portland, OR 2007. Zob. także P. Dąbrowska, *Równoważenie ochrony i rozwiązywanie konfliktów — orzecznictwo ETS w sporach dotyczących praw podstawowych i rynku wewnętrznego (swoboda przepływu osób i świadczenia usług)*, [w:] *Przepływ osób i świadczenie usług w Unii Europejskiej*, red. S. Biernat, S. Dudzik, Warszawa 2009; oraz wyroki TSUE w sprawach C-112/00 *Eugen Schmidberger, Internationale Transporte und Planzüge przeciwko Republik Österreich* [2003] ECR I 5659; C-36/02 *Omega Spielhallen- und Automatenaufstellungs-GmbH przeciwko Oberbürgermeisterin der Bundesstadt Bonn* [2004] ECR I-09609.

[6] Zob. Council Conclusions of 13 September 2010 on lessons learned from the A/H1N1 pandemic — health security in the European Union, nr dokumentu 12665/10; oraz Presidency Conclusions of 15 November 2001 on Bioterrorism, nr dokumentu 13826/01.

[7] Zob. D.P. Fidler, *From International Sanitary Conventions to Global Health Security: The New IHR*, „Chinese Journal of International Law" 4 (325), 2005; L.O. Gostin, *Global Health Law*, Cambridge, MA 2014.

przez organy ochrony zdrowia (część 3); podstawowe narzędzia i środki regulacyjne ustanowione decyzją 1082/2013 w zakresie przeciwdziałania i reagowania na poważne zagrożenia dla zdrowia publicznego na szczeblu unijnym (część 4); przepisy i środki szczególne służące zabezpieczeniu ochrony danych osobowych przekazywanych w trakcie uruchamiania unijnego systemu wczesnego ostrzegania i reagowania (część 5). W podsumowaniu (część 6), znajdują się wnioski *de lege lata* i *de lege ferenda* dotyczące obecnego systemu ochrony danych osobowych w kontekście stosowania postanowień o zagrożeniach dla zdrowia publicznego. Głównym celem pracy jest zbadanie, czy przepisy i środki chroniące wartości będące w potencjalnym konflikcie w sytuacji transgranicznego zagrożenia, czyli prawo do ochrony danych osobowych oraz bezpieczeństwo publiczne, tworzą spójny i kompletny system, i czy w konsekwencji mogą być efektywnie stosowane. W opracowaniu pominięto te kwestie kompetencyjne oraz instytucjonalne, które nie mają kluczowego znaczenia dla zrozumienia konfliktu między ochroną zdrowia a ochroną danych osobowych jednostek przy stosowaniu prawa UE o zagrożeniach dla zdrowia (np. procedura wspólnych zamówień na produkty medyczne w kontekście przypadków sytuacji nadzwyczajnych).

Zastosowana w badaniach metodologia prawnicza objęła analizę tekstów prawnych, orzecznictwa i dokumentów instytucjonalnych w świetle aktualnej literatury przedmiotu. W szczególności zastosowano dogłębną analizę relewantnych aktów prawnych oraz opisów praktyki działania omawianych instytucji, uzyskanych na podstawie dostępnych dokumentów instytucji unijnych (sprawozdania Komisji, opinie Europejskiego Inspektora Ochrony Danych Osobowych — „EIOD", strony internetowe *DG SANTE* i ECDC).

2. PRAWO DO OCHRONY DANYCH OSOBOWYCH W UE — ZARYS

Unijne prawo podstawowe do ochrony danych osobowych wynika wprost z art. 8 Karty Praw Podstawowych (KPP)[8]. W unijnym systemie prawnym jest to prawo wyszczególnione w relacji do prawa do prywatności z art. 7 KPP[9]. W świetle KPP nie jest to prawo absolutne, ponieważ może podlegać ograniczeniom zgodnie z art. 52 i interpretacją Trybunału Sprawiedliwości UE, który w tym kontekście cytuje też często orzecznictwo Europejskiego Trybunału Praw Człowieka wydane przy wykładni art. 8 ust. 2 EKPCz[10]. Ograniczeniu może podlegać także prawo

[8] Por. Agencja Praw Podstawowych UE i Rada Europy, *Podręcznik europejskiego prawa o ochronie danych*, Urząd Publikacji UE, Luksemburg 2014, s. 18–22.

[9] Por. np. *Komentarz do Karty Praw Podstawowych*, red. A Wróbel, Warszawa 2012. Zob. A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości*, Warszawa 2015.

[10] Por. wyroki TSUE w sprawach połączonych C-465/00, C 138/01 i C 139/01 *Österreichischer Rundfunk i inni* [2003] ECR I 4989 oraz C-92/09 i C-93/09 *Volker i Markus Schecke GbR oraz*

do ochrony danych dotyczących zdrowia, tym niemniej — jak wyjaśnia TSUE — tylko w ściśle określonych przypadkach:

> Zgodnie z orzecznictwem Trybunału prawo do poszanowania życia prywatnego, ustanowione w art. 8 EKPC i wynikające ze wspólnej tradycji konstytucyjnej państw członkowskich, stanowi jedno z praw podstawowych chronionych przez porządek prawny Unii. Obejmuje ono między innymi prawo osoby do zachowania swego stanu zdrowia w tajemnicy […].
>
> Przekazanie osobie trzeciej, w tym innej instytucji, danych osobowych dotyczących stanu zdrowia tej osoby zgromadzonych przez daną instytucję stanowi samo w sobie ingerencję w życie prywatne zainteresowanej osoby, bez względu na to, jak zostaną następnie użyte informacje w ten sposób przekazane […].
>
> Jednak zgodnie z orzecznictwem ograniczenia praw podstawowych mogą być uzasadnione, jeśli faktycznie odpowiadają nadrzędnym względom interesu ogólnego i nie stanowią — w świetle zamierzonego celu — nieproporcjonalnej i niemożliwej do zniesienia ingerencji, która naruszałaby samą treść tak gwarantowanego prawa […]. W tym względzie za punkt odniesienia służy art. 8 ust. 2 EKPC. Zgodnie z tym przepisem ingerencja władzy publicznej w życie prywatne może być uzasadniona tylko w zakresie: i) przypadków „przewidzianych przez ustawę", ii) gdy służy jednemu lub kilku wymienionym celom oraz iii) gdy jest „konieczna" do osiągnięcia tego celu lub celów[11].

Zgodnie z powyższą wykładnią ingerencja w prawo do ochrony danych medycznych jest dopuszczalna, gdy zastosowane zostaną enumeratywne wyjątki z prawa wtórnego, oraz gdy realizuje cel prawnie uregulowany i jest zgodna z zasadą proporcjonalności UE.

Uregulowanie ochrony danych w prawie wtórnym jest gwarantowane przez dyrektywę 95/46, która wprowadza harmonizację całkowitą prawa krajowego państw członkowskich[12]. Od 25 maja 2018 roku akt ten zostanie zastąpiony przez nowe rozporządzenie 2016/679[13]. Z kolei przepisy regulujące ochronę danych osobowych przez instytucje UE zapewnia rozporządzenie 2001/45[14]. Dyrektywa, która zawiera przepisy szczególne wobec art. 8 KPP, szczegółowo normuje zasady

---

Hartmut Eifert przeciwko Land Hessen [2010] ECR I-11063. Zob. także wyroki ETPCz w sprawach Amann v Switzerland [GC], no. 27798/95, § 65, ECHR 2000 II; Rotaru v Romania [GC], no. 28341/95, § 43, ECHR 2000 V.

[11] F-46/09 *V przeciwko Parlamentowi Europejskiemu*, ECLI:EU-:F:2011:101, par. 112–114.

[12] Zob. dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE 1995, L 281/31; oraz wyrok TSUE w sprawie C-101/01 *Postępowanie karne przeciwko Bodil Lindqvist* [2003] I-12971, par. 96.

[13] Art. 94 i 99 rozporządzenia (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE 2016, L 119/1. Por. *Reforming European data protection law*, red. S. Gutwirth, R. Leenes, P. de Hert, Dordrecht 2015.

[14] Zob. rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz. Urz. UE 2001, L 8/1.

legalnego przetwarzania i przechowywania danych oraz prawo do dostępu i korekty danych przez jednostkę, której one dotyczą[15].

Zakres przedmiotowy prawa do ochrony danych obejmuje wszelkie dane identyfikujące lub pozwalające na identyfikację osoby. Zwiększonej ochronie prawnej podlegają tzw. szczególne kategorie danych, np. ujawniające pochodzenie etniczne lub rasowe oraz dotyczące zdrowia danej jednostki[16]. Przetwarzanie tych kategorii danych jest zatem możliwe tylko z zastosowaniem szczególnych zabezpieczeń, ponieważ w świetle prawa wtórnego UE przetwarzanie danych szczególnie wrażliwych jest co do zasady zabronione (art. 8 ust. 1 dyrektywy 95/46). Art. 9 ust. 1 nowego rozporządzenia 2016/679, które będzie mieć zastosowanie od 25 maja 2018 roku, zawiera analogiczny zakaz.

Wyjątki od ogólnego zakazu przetwarzania danych osobowych dotyczących zdrowia obejmują następujące wyłączenia: wyraźna zgoda podmiotu danych, żywotne interesy osoby, której dane dotyczą, uzasadnione interesy innych osób i interes publiczny[17]. W kontekście niniejszego tekstu szczególne znaczenie i podstawowe zastosowanie ma wyjątek z art. 8 ust. 3 dyrektywy 95/46, który wyłącza ogólny zakaz przetwarzania danych dotyczących zdrowia, nawet bez zgody osoby, której dane dotyczą:

> jeżeli przetwarzanie danych wymagane jest do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane są przetwarzane przez pracownika służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegającemu obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy.

Analogiczny wyjątek przewiduje art. 9 ust. 2 litera i) rozporządzenia 2016/679, który został wyraźnie dostosowany do nowych przepisów unijnych o transgranicznych zagrożeniach dla zdrowia. Ogólny zakaz przetwarzania danych dotyczących zdrowia nie ma zastosowania, gdy:

> przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

---

[15] Por. szerzej np. *Podręcznik europejskiego prawa…*, s. 65–134 lub O. Lynskey, *The foundations of EU data protection law*, Oxford 2015.

[16] *Podręcznik europejskiego prawa…*, s. 42–45; por. wyroki w sprawach C-404/92 *P X przeciwko Komisji* [1994] I-04737; i F-46/09 *V przeciwko Parlamentowi Europejskiemu*, ECLI:EU:F:2011:101.

[17] *Podręcznik europejskiego prawa…*, s. 92–93.

Warto zaznaczyć, że w cytowanych przypadkach unormowań dyrektywy 95/46 i rozporządzenia 2016/679 szczególnym zabezpieczeniem ochrony prawa jest fakt, że podmioty dokonujące przetworzenia danych powinny być objęte obowiązkiem zachowania tajemnicy zawodowej[18].

Przed opisem studium przypadku pozwalającym zrozumieć istotę stosowania przepisów o ochronie zdrowia i ochrony danych warto wskazać podstawowe konsekwencje zastosowania wyjątków od zakazu przetwarzania danych zdrowotnych, nawet w granicach prawa: przekazywania danych medycznych bez możliwości wyrażenia świadomej zgody, dalszego ograniczania praw podstawowych w postaci odmowy wejścia na pokład linii lotniczych lub stosowania środków detencyjnych, np. kwarantanny[19].

3. „GRUŹLIK-PODRÓŻNIK" A EUROPEJSKI SYSTEM WCZESNEGO OSTRZEGANIA I REAGOWANIA — STUDIUM PRZYPADKU

W jednym z publicznie dostępnych sprawozdań z roku 2009 z działania Europejskiego Systemu Wczesnego Ostrzegania i Reagowania (EWRS) można przeczytać, że jednym ze zgłoszonych zagrożeń zdrowia był „przypadek obywatela Amerykańskiego podróżującego po Europie, u którego zdiagnozowano XDR-TB (*extensively drug-resistant tuberculosis* — całkowicie lekooporna gruźlica)" notyfikowanego dnia 25 maja 2008 roku przez władze włoskie ds. ochrony zdrowia[20].

Pacjent przybył do UE lotem transoceanicznym z Atlanty do Paryża, a następnie powrócił do Ameryki Północnej lotem Czech Airlines z Pragi do Montrealu w Kanadzie, aby wjechać z powrotem do Stanów Zjednoczonych samochodem. Osoba ta została zdiagnozowana jako zarażona gruźlicą w marcu i była poinformowana podczas podróżowania po Europie, że choruje na przypadek choroby całkowicie lekoopornej. Zgodnie z oceną ryzyka dokonaną przez unijną ECDC poziom zakaźności tego pacjenta był bardzo niski i nie było dowodu, aby ten rodzaj XDR-TB był bardziej zaraźliwy od normalnego szczepu gruźlicy. Jednak w związku z powagą zagrożenia całkowicie lekoopornym szczepem choroby ECDC zaleciła jako środek przezorności zastosowanie wytycznych Światowej Organizacji Zdrowia „Gruźlica w Podróżach Lotniczych" dla obu lotów transatlantyckich

[18] Por. *ibidem*, s. 94.

[19] Zob. w tym kontekście P. Złamańczuk, *Pozbawienie wolności w celu zapobieżenia szerzeniu choroby zakaźnej w świetle Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, „Prawo i Medycyna" 2016, nr 62, s. 14–31.

[20] Report from the Commission on the Operation of the Early Warning and Response System (EWRS) of the Community Network for the epidemiological surveillance and control of communicable diseases during 2006 and 2007 (Decision 2000/57/EC), COM(2009) 228 final, s. 5 (dalej: Sprawozdanie 2009).

(trwających ponad 8 godzin), gdzie pacjent był pasażerem[21]. Komisja Europejska zorganizowała i przewodniczyła licznym spotkaniom z zainteresowanymi państwami członkowskimi, agencją ECDC, ŚOZ, Stanami Zjednoczonymi, Kanadą i przedstawicielstwami Komisji w USA i Kanadzie. Uzgodniono zastosowanie działań mających na celu tzw. ustalenie kontaktów zakaźnych, czyli dotarcie do wszystkich pasażerów problematycznych lotów i ustalenie ich dalszych kontaktów z powiadomieniem o ryzyku choroby[22]. W międzyczasie amerykańskie media przekazywały na bieżąco wszelkie informacje i sensacje dostępne na temat podróży, okoliczności, rodziny i stanu zdrowia pana Andrew Speakera, który po powrocie do Stanów został zatrzymany i poddany przymusowej kwarantannie[23].

Przypadek ten został uznany przez instytucje UE i zainteresowane państwa członkowskie za szczególnie istotny z punktu widzenia potrzeby wzmocnienia istniejącego mechanizmu ustalania kontaktów zakaźnych w UE[24]. W raporcie EWRS wskazano dodatkowo, że cała historia przypadku pana Speaker'a (który *nota bene* w dokumentach europejskich zawsze występuje jako anonimowy przypadek) spowodowała konieczność zwrócenia uwagi na następujące kwestie w unijnej ochronie zdrowia: (i) problemy dotyczące ochrony danych osobowych; (ii) możliwość stworzenia unijnej listy osób „z zakazem lotu"; (iii) odpowiedzialność linii lotniczych i biur podróży za gromadzenie, udostępnianie i przechowywanie danych osobowych podróżnych dla celów środków ochrony zdrowia publicznego, takich jak ustalanie kontaktów zakaźnych; (iv) przekazywanie danych pasażerów do krajowych organów ochrony zdrowia; (v) wdrażanie procedury ustalania kontaktów zakaźnych tylko dla przypadków gruźlicy wielolekoopornej i całkowicie lekoopornej (MDR-TB i XDR-TB)[25].

Można uznać, że historia pana Speakera w kontekście europejskim zadziałała jak swego rodzaju efekt destabilizujący (*destabilisation efect*) dla regulacji[26]. Równolegle z coraz częściej pojawiającymi się epidemiami o zasięgu regionalnym lub globalnym przypadek ten przyczynił się do przyspieszenia reformy i unowocześnienia unijnego systemu reagowania na zagrożenia dla zdrowia publicznego

---

[21] Zob. WHO, *Tuberculosis and air travel, Guidelines for prevention and control*, WHo/HTM/TB/2008.399, wyd. 3, Geneva 2008, wyd. poprawione 2013. Por. też wiadomość prasowa WHO, *WHO report warns global actions and investments to end tuberculosis epidemic are falling far short*, 13.10.2016; *WHO Global Tuberculosis Report 2016*, WHO/HTM/TB/2016.1, Geneva 2016.

[22] Zob. też w tym kontekście Art. 1 Międzynarodowe Przepisy Zdrowotne (dalej: MPZ), 2005, http://www.who.un.org.pl/aktualnosci.php?news=106&wid=14&wai=&year=&back=%2Faktualnosci.php%3Fwid%3D14 (dostęp: 14.10.2016). Por. też L.O. Gostin, D.P. Fidler, *Biosecurity in the Global Age: Biological Weapons, Public Health, and the Rule of Law*, Stanford, California 2007.

[23] Zob. H.A. Fallow, *Reforming Federal Quarantine Law in the Wake of Andrew Speaker: "The Tuberculosis Traveler"*, „Journal of Contemporary Health Law & Policy" 25 (1), 2008, s. 83–106.

[24] Sprawozdanie 2009, s. 5.

[25] *Ibidem*, s. 6.

[26] Por. C.F. Sabel, J. Zeitlin, *Experimentalist Governance*, [w:] *Oxford Handbook on Governance*, red. D. Levi-Faur, Oxford 2012, s. 167–184.

oraz ochrony danych medycznych w tym kontekście[27]. W efekcie w 2009 roku Komisja Europejska przedstawiła projekt decyzji o poważnych, transgranicznych zagrożeniach zdrowia, który ostatecznie został przyjęty w 2013 roku. Akt ten jest głównym przedmiotem analizy w niniejszym tekście.

4. NARZĘDZIA REGULACYJNE UE PRZECIWDZIAŁAJĄCE POWAŻNYM TRANSGRANICZNYM ZAGROŻENIOM DLA ZDROWIA W ŚWIETLE DECYZJI 1082/2013

Decyzja 1082/2013 realizuje cel przeciwdziałania zagrożeniom dla zdrowia na poziomie UE przez ustanowienie określonych sposobów, narzędzi regulacyjnych i rozwiązań instytucjonalnych[28]. Niektóre z nich są nowe (np. możliwość wspólnych zamówień państw na środki medyczne), lecz większość to skonsolidowanie, rozszerzenie zakresu i kontynuacja rozwiązań istniejących (np. nadzór epidemiologiczny) oraz nadanie dotychczas nieformalnie działającym strukturom instytucjonalnym ram prawnych, np. Komitetowi ds. Bezpieczeństwa Zdrowia[29]. Ten ostatni odgrywa istotną rolę we wdrażaniu i stosowaniu decyzji 1082/2013, i składa się z przedstawicieli państw członkowskich, którzy koordynują działania na poziomie UE i reprezentują właściwe organy państw członkowskich ds. zdrowia publicznego. Ponadto Komisję wspomaga tzw. komitet komitologiczny (Komitet ds. Poważnych Transgranicznych Zagrożeń Zdrowia) oraz ECDC[30].

Według obecnego stanu prawnego na mocy decyzji 1082/2013 podstawowe sposoby przeciwdziałania poważnym transgranicznym zagrożeniom dla zdrowia to: planowanie gotowości i koordynacja reagowania, wczesne ostrzeganie przez wymianę informacji, w tym ustalanie kontaktów zakaźnych, nadzór epidemiologiczny, monitorowanie, w tym monitorowanie doraźne, ogłaszanie sytuacji nadzwyczajnych. Sposoby te są realizowane przede wszystkim za pośrednictwem szczególnych narzędzi regulacyjnych ustanowionych na poziomie UE, tj.: „sieci nadzoru epidemiologicznego" (art. 6) oraz „systemu wczesnego ostrzegania i reagowania" (EWRS, art. 8) i specyficznych aktów administracyjnych wywołujących skutki prawne, tj. „ostrzeżenie/powiadomienie" (art. 9). ECDC obsługuje

---

[27] Por. H.A. Fallow, *op. cit.*; Sprawozdanie 2009, s. 6.

[28] Por. szerzej S. Brem, S. Dubois, *Different Perceptions, Similar Reactions: Biopreparedness in the European Union*, [w:] *Global Biosecurity Threats and Responses*, red. P. Katona, J.P. Sullivan, M.D. Intriligatore, Oxon-New York 2010, s. 137–156.

[29] Por. M.L. Flear, *Governing Public Health: EU Law, Regulation and Biopolitics*, Oxford-Portland, OR 2015, s. 144 n.

[30] Art. 17–18 decyzji 1082/2013; oraz rozporządzenie (UE) nr 182/2011 ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję, Dz. Urz. 2011, L 53/13.

i koordynuje sieć nadzoru epidemiologicznego, jak również prowadzi EWRS[31]. Natomiast ostrzeżenia wydają, czy też wysyłają w ramach EWRS, organy krajowe lub Komisja.

4.1. NADZÓR EPIDEMIOLOGICZNY

Unijny nadzór epidemiologiczny to zbieranie, analizowanie i przetwarzanie danych oraz statystyk dotyczących chorób zakaźnych, w tym analiza ryzyka. Jest on realizowany za pośrednictwem platform internetowych wymiany informacji o ograniczonym dostępie (zabezpieczone hasłem) z uwagi na przechowywane tam dane, choć obie bazy danych przechowywanych na serwerze ECDC zawierają jedynie zanonimizowane dane osobowe, czyli takie, które nie pozwalają na zidentyfikowanie indywidualnej osoby[32].

Obecnie ECDC prowadzi nadzór epidemiologiczny nad 52 chorobami zakaźnymi, o których informacje przekazują państwa członkowskie za pośrednictwem wspomnianych platform wymiany informacji: TESSy i EPIS[33]. „TESSy jest platformą techniczną do prowadzenia nadzoru nad chorobami zakaźnymi w UE/EOG, tj. platformą służącą do przekazywania danych za pośrednictwem internetu, przechowywania danych i ich rozpowszechniania; […]”[34]. TESSY służy głównie do nadzoru epidemiologicznego w oparciu o wskaźniki (*indicator-based*), na podstawie których ECDC generuje m.in. dzienne, tygodniowe, miesięczne i roczne raporty dla poszczególnych chorób i zagrożeń, ogólnodostępne bazy danych o chorobach zakaźnych, artykuły naukowe itp. Natomiast EPIS (*Epidemic Intelligence Information System*) — w pewnym uproszczeniu — to narzędzie wywiadu epidemiologicznego w oparciu o analizę zdarzeń (*event-based*), mający na celu przede wszystkim określenie wpływu potencjalnego zagrożenia na rozwój chorób na terenie UE/EOG. W oparciu o posiadane dane ECDC przygotowuje cotygodniowy raport ryzyka chorób zakaźnych (*Communicable Disease Threats Report*) — zbiorowy dla różnych jednostek chorobowych i publikowany na stronie ECDC[35].

---

[31] Punkt 5 preambuły, art. 6 i 9, decyzja 1082/2013; art. 8, rozporządzenie 851/2004. Zob. http://ecdc.europa.eu/en/aboutus/what-we-do/surveillance/Pages/index.aspx (dostęp: 21.10.2016).

[32] Por. *Podręcznik europejskiego prawa…*, s. 45. Z uwagi na główny wątek tego tekstu instytucja nadzoru jest w niniejszej pracy przedstawiona skrótowo.

[33] Zob. decyzję Komisji 2009/312/WE zmieniającą decyzję 2000/96/WE w odniesieniu do wyspecjalizowanych sieci nadzoru nad chorobami zakaźnymi, Dz. Urz. WE 2009, L 91/27.

[34] Sprawozdanie Komisji dotyczące wdrożenia decyzji Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylającej decyzję nr 2119/98/WE, COM(2015) 617 final, s. 8 (dalej: Sprawozdanie 2015).

[35] Zob. np. raport dot. 9–15 października 2016 r., http://ecdc.europa.eu/en/publications/Publications/communicable-disease-threats-report-15-oct-2016.pdf (dostęp: 20.10.2016).

4.2. SYSTEM WCZESNEGO OSTRZEGANIA I REAGOWANIA (EWRS)

„System wczesnego ostrzegania i reagowania" jest obecnie ustanowionyw art. 8 decyzji 1082/2013 (który zastępuje mechanizm wprowadzony we wcześniejszej regulacji decyzją 2119/98/WE), a szczegółowe procedury dotyczące prawidłowego funkcjonowania EWRS, jednolitego wdrażania przepisów unijnych, są uregulowane w aktach wykonawczych Komisji. Większość z nich przyjęto jeszcze podczas obowiązywania decyzji 2119/98/WE, która została zastąpiona przez decyzję 1082/2013 i dotyczy wymiany informacji tylko w zakresie chorób zakaźnych, podczas gdy obecny zakres przedmiotowy regulacji jest szerszy, a zatem przepisy te powinny podlegać stopniowej aktualizacji[36]. Nadrzędnym celem działania takiego systemu jest natychmiastowa, kompetentna i bezpośrednia komunikacja między Komisją i właściwymi unijnymi agencjami a państwami członkowskimi w celu przekazywania ostrzeżeń w sytuacji wystąpienia ryzyka poważnych transgranicznych zagrożeń dla zdrowia publicznego.

System ten zapewnia stałą łączność między Komisją a właściwymi rzeczowo organami krajowymi państw członkowskich, które opowiadają za ostrzeganie w przypadku zagrożenia dla zdrowia, oceniają ryzyko zagrożenia na poziomie krajowym oraz określają środki konieczne do podjęcia, aby tym zagrożeniom zapobiegać. Wymiana wszelkich informacji następuje drogą elektroniczną przez narzędzie informatyczne prowadzone i zarządzane, podobnie jak nadzór epidemiologiczny, przez ECDC[37]. Zatem operacyjnie EWRS stanowi platformę elektroniczną o dostępie ograniczonym dla uprawnionych instytucji z uwagi na możliwy przepływ danych osobowych i innych wrażliwych informacji dotyczących bezpieczeństwa zdrowia publicznego. Organy uprawnione to właściwe urzędy ds. ochrony zdrowia publicznego państw członkowskich, desygnowane przez rządy państw członkowskich na członków EWRS, oraz właściwa część dyrekcji Komisji ds. zdrowia (SANTE), np. *Health Threats Unit*[38].

Państwa członkowskie są zobowiązane do wskazania organów uprawnionych do działań na mocy decyzji 1082/2013. Są to zazwyczaj właściwe, krajowe organy ochrony zdrowia (w Polsce: Główny Inspektorat Sanitarny w strukturze Ministerstwa Zdrowia). Po wskazaniu organu Komisja przekazuje login i hasło wraz z upoważnieniem o pełnym dostępie do obu funkcji systemu: czytania i komentowania wiadomości. Od sierpnia 2015 r. dostęp do EWRS przyznawany jest za pośrednictwem systemu uwierzytelniania Komisji Europejskiej (ECAS) przez spersonalizowane adresy e-mail i hasła[39].

---

[36] Art. 8 i 20 decyzji 1082/2013 oraz akty prawne dostępne: http://ec.europa.eu/health/communicable_diseases/early_warning/comm_legislation_en.htm (dostęp: 21.10.2016)

[37] Art. 8 ust. 1, rozporządzenie (WE) 851/2004.

[38] https://ewrs.ecdc.europa.eu/ (dostęp: 25.10.2016)

[39] Art. 15 ust. 1, decyzja 1082/2013. Por. Report form the Commission on the operation of the Early Warning and Response Systems (EWRS) of the Community Network for the epidemiological

4.3. OSTRZEŻENIE Z ART. 9 DECYZJI 1082/2013

Podstawowym obowiązkiem właściwych organów krajowych lub Komisji w ramach sieci kontaktów jest „powiadamianie o zagrożeniu za pośrednictwem EWRS", gdy pojawienie się lub rozwój poważnego transgranicznego zagrożenia dla zdrowia spełnia kumulatywnie określone w decyzji kryteria[40]. Można je sklasyfikować według: (1) zasięgu terytorialnego — „oddziałuje lub potencjalnie może oddziaływać na więcej niż jedno państwo członkowskie"; (2) zasady subsydiarności — „wymaga albo może wymagać" podjęcia skoordynowanych działań na poziomie UE; (3) prawdopodobieństwa wysokiego ryzyka — co wynikać może z czterech różnych czynników: charakteru zdarzenia, poziomu zakaźności/umieralności, tempa rozwoju lub rozmiaru[41]. Czynniki dotyczące oceny ryzyka (oceny naukowej) zdarzenia są określone alternatywnie: „a) ma charakter nadzwyczajny lub niespodziewany dla danego miejsca i czasu lub powoduje bądź może powodować znaczną zachorowalność lub umieralność u ludzi lub rozwija się szybko bądź może rozwijać się szybko lub wykracza bądź może wykraczać poza krajowe możliwości reagowania; […]"[42].

Zakres informacji, które organy są zobowiązane przekazać, jest możliwie najszerszy i obejmuje „wszelkie dostępne informacje, które mogą być przydatne" dla efektywnego skoordynowania reagowania. Decyzja zawiera przykładowe wyliczenie informacji koniecznych do pełnej charakterystyki zdarzenia i możliwości zorganizowania odpowiednich działań (np. rodzaj, pochodzenie choroby, czas i miejsce wystąpienia, sposoby przenoszenia, metody wykrywania, środki ochrony już podjęte), w tym — co jest najbardziej istotne z punktu widzenia niniejszego tekstu — dane osobowe niezbędne do tzw. ustalenia kontaktów zakaźnych, a także wszelkie inne informacje istotne dla danego zagrożenia, które teoretycznie mogą również obejmować osobowe dane medyczne[43]. Obowiązek przekazania odnośnych informacji przez EWRS powstaje również, jeżeli władze krajowe uruchamiają procedurę powiadamiania w ramach art. 6 Międzynarodowych Przepisów Zdrowotnych. Dzięki horyzontalnemu charakterowi sieci informacyjnej i narzędziom elektronicznym informacje docierają jednocześnie do wszystkich państw członkowskich UE i Komisji lub, jeżeli wymaga tego ochrona danych osobowych, tylko do wybranych, zainteresowanych państw[44].

---

surveillance and control of communicable diseases during years 2004 and 2005 (Decision 2000/57/EC), COM(2007) 121 final, s. 1 (dalej: Sprawozdanie 2007); Sprawozdanie 2015, s. 8.

[40] Art. 9 ust. 1 decyzji 1082/2013. Zob. też art. 4 rozporządzenia 851/2004.

[41] Art. 9 ust. 1 decyzji 1082/2013.

[42] Art. 9 ust. 1 pkt a) decyzji 1082/2013. Por. też załącznik I do decyzji 57/2000 ze zmianami, który wcześniej określał przypadki dotyczące obowiązku zgłaszania w ramach EWRS w odniesieniu do chorób zakaźnych, i na razie nie został formalnie uchylony.

[43] Art. 9 ust. 3, punkty i)–j). Zob. *Podręcznik europejskiego prawa…*, s. 92.

[44] Art. 16 ust. 3 decyzji 1082/2013.

Zakresem przedmiotowym pojęcia „poważnych transgranicznych zagrożeń" są obecnie objęte: zagrożenia biologiczne, w tym choroby zakaźne; oporność na środki przeciwdrobnoustrojowe i zakażenia związane z opieką zdrowotną; biotoksyny czy inne szkodliwe czynniki biologiczne; następnie zagrożenia o pochodzeniu chemicznym, środowiskowym czy „nieznanym"; oraz wszelkie nadzwyczajne sytuacje w dziedzinie zdrowia o zasięgu międzynarodowym dotyczące powyższych kategorii zgodnie z Międzynarodowymi Przepisami Zdrowotnymi[45]. Tę ostatnią kategorię należy rozumieć jako odwołanie do sytuacji, kiedy ŚOZ ogłasza przypadek stanu zagrożenia zdrowia publicznego o znaczeniu międzynarodowym (ang. *international health emergencies*)[46].

Katalog zagrożeń jest szeroki i otwarty, dotyczy bowiem nie tylko bezpośredniego zagrożenia chorobami wywoływanymi przez bakterie czy wirusy, lecz także przypadków lekooporności czy zakażeń poszpitalnych występujących przy okazji leczenia chorób zakaźnych, np. dodatkowych zakażeń bakteriami salmonella, oraz możliwych zagrożeń nieznanych. „Transgraniczność" i „powaga" zagrożenia są także szeroko zdefiniowane i oznaczają „zagrażające życiu lub w innym stopniu poważne" ryzyko, które się rozprzestrzenia lub może rozprzestrzeniać poza granice państw członkowskich i tym samym wymagać reakcji oraz działań na szczeblu unijnym. Zagrożenia mogą być zarówno naturalne, jak i wynikać z działalności człowieka, np. bioterroryzm[47]. W efekcie nowy system poszerza zakres przedmiotowy EWRS w stosunku do regulacji z końca lat 90., która dotyczyła pierwotnie tylko chorób zakaźnych, co może mieć wpływ na możliwość utrzymania wysokiego poziomu ochrony danych osobowych (zobacz niżej)[48].

W tym celu rozszerzono istniejące narzędzie informatyczne EWRS, aby uwzględnić zagrożenia biologiczne, chemiczne, środowiskowe i o nieznanym pochodzeniu. Nową wersję tego narzędzia informatycznego wprowadzono w dniu 4 lutego 2015 r. Kryteria pozwalające sprawdzić, czy dane zdarzenie pasuje do definicji „poważnego transgranicznego zagrożenia zdrowia", zostały uwzględnione w algorytmie sprawozdawczym; dodano też specjalną funkcję zgłaszania „komunikatów informacyjnych" oraz funkcję zgłaszania zdarzenia zgodnie z IHR. Funkcję „komunikacji selek-

[45] Art. 2 ust. 1; art. 3 punkt g) decyzji 1082/2013. Zob. też Konkluzje Rady w sprawie następnych kroków w dziedzinie zwalczania oporności na środki przeciwdrobnoustrojowe w ramach podejścia „Jedno zdrowie", Dz. Urz, UE 2016, C 269/26.

[46] Por. art. 1 ust. 1 MPZ. Zob. też. http://www.who.int/emergencies/en/ (dostęp: 21.10.2016).

[47] Zob. punkt 4 preambuły decyzji 1082/2013 i np. F. Kuhlau, *Countering Bio-Threats: EU Instruments for Managing Biological Materials, Technology and Knowledge*, „SIPRI Policy Paper" 2007, nr 19; oraz G.D. Koblentz, *Living weapons: biological warfare and international security*, Ithaca-London 2009.

[48] Por. poprzednio obowiązującą decyzję Nr 2119/98/WE Parlamentu Europejskiego i Rady z dnia 24 września 1998 r. ustanawiająca sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie, Dz. Urz. UE 1998, L 268/1; oraz Sprawozdanie 2015, punkt 2.5. s. 8 i Streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Parlamentu Europejskiego i Rady w sprawie poważnych transgranicznych zagrożeń zdrowia z 28 marca 2012 roku, Dz. Urz. UE 2012 C 197/21, pkt 4.

tywnej" zachowano bez zmian, w kształcie, w jakim istniała w aplikacji informacyjnej utworzonej na mocy decyzji nr 2119/98/WE[49].

Istnieją trzy poziomy powiadomień w ramach EWRS w zależności od poziomu ryzyka: (1) wymiana informacji; (2) potencjalne zagrożenie; i (3) pewne zagrożenie. Każdemu poziomowi zagrożenia odpowiadają odpowiednie obowiązki organów państw członkowskich i Komisji[50]. W sytuacji powiadomień poziomu 2 i 3 istnieje też narzędzie powiadamiania SMS-owego personelu Komisji w celu zwiększenia efektywności komunikacji[51].

Warto też zauważyć, że narzędzie to w założeniu ma uzupełniać, a nie powielać dotychczas już istniejące na poziomie UE systemy monitorowania i ostrzegania przed zagrożeniami dla zdrowia dotyczącymi bądź to szczególnego rodzaju działalności (zagrożenia radiologiczne, jądrowe), bądź określonego rodzaju towarów, np. sieć systemu wczesnego ostrzegania o niebezpiecznej żywności i paszach (RASFF) funkcjonująca dla zapewnienia bezpieczeństwa żywności na podstawie Ogólnego Prawa Żywnościowego[52].

4.4. MOŻLIWE SKUTKI PRAWNE OSTRZEŻENIA Z ART. 9 DECYZJI 1082/2013

Wysłanie ostrzeżenia na podstawie art. 9 decyzji 1082/2013 w ramach systemu EWRS przez właściwy organ państwa członkowskiego ma wiele skutków prawnych na płaszczyźnie prawa unijnego i — w określonych przypadkach — prawa krajowego.

4.4.1. OCENA RYZYKA

Po pierwsze, jest przeprowadzana ocena ryzyka przez Europejskie Centrum ds. Zapobiegania i Kontroli Chorób, Europejski Urząd ds. Bezpieczeństwa Żywności lub inną właściwą agencję UE w zależności od zakresu uprawnień danej instytucji. ECDC analizuje na bieżąco treść otrzymywanych komunikatów, zapewnia też fachową wiedzę i doradztwo za pośrednictwem zatrudnianych lub zewnętrznych ekspertów[53]. Przeprowadzona ocena ryzyka jest bezzwłocznie udostępniana właściwym organom krajowym i KBZ przez Komisję, która przekazuje także informacje o możliwych do zastosowania środkach w zakresie zdrowia publicznego w każdej sytuacji powiadomienia poprzez system EWRS (na podstawie art. 9 decyzji 1082/2013), gdy jest to niezbędne dla koordynacji w ramach UE albo gdy

[49] Sprawozdanie 2015, s. 8.

[50] Załącznik II, decyzja 2000/57/WE. Zob. też sprawozdanie 2015, s. 9.

[51] Sprawozdanie 2007.

[52] Zob. art. 50 rozporządzenia (WE) 178/2002 ustanawiającego ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności, Dz. Urz. 2002 L 31/1.

[53] Art. 8 ust. 2 rozporządzenia 851/2004. Zob. też M. Górka [w:] J. Barcz, M. Górka, A. Wyrozumska, *Instytucje i prawo Unii Europejskiej*, wyd. 4, Warszawa 2015.

Komisja decyduje tak z własnej inicjatywy lub na wniosek KBZ[54]. Ocena ryzyka jest udostępniana poprzez EWRS także w przypadku, gdy jest ona przeprowadzana doraźnie przez Komisję z tego powodu, że jej zakres jest poza kompetencjami właściwych unijnych agencji (art. 10 ust. 2 rozporządzenia 251/2004)[55].

4.4.2. MONITOROWANIE DORAŹNE

W przypadku zagrożeń innych niż choroby zakaźne istnieje dodatkowo instytucja „monitorowania doraźnego" (art. 7 decyzji 1082/2013) uruchamiana w przypadku zagrożenia biotoksycznego, chemicznego, środowiskowego lub nieznanego wraz z powiadomieniem w ramach EWRS z art. 9. Narzędzie to pełni funkcję swego rodzaju nadzoru epidemiologicznego *ad hoc*, oznacza bowiem obowiązek wzajemnego informowania się państw członkowskich w porozumieniu z Komisją za pośrednictwem EWRS lub za pośrednictwem KBZ o rozwoju zagrożenia na szczeblu krajowym na podstawie posiadanych informacji z wewnętrznych systemów monitorowania. Zakres przekazywanych informacji obejmuje według wyliczenia przykładowego „wszelkie zmiany w zakresie rozmieszczenia geograficznego, rozprzestrzeniania się i nasilenia oraz metod wykrywania zagrożenia"[56].

4.4.3. OBOWIĄZEK WYMIANY INFORMACJI I KOORDYNACJI DZIAŁAŃ

Ostrzeżenie z art. 9 może skutkować także obowiązkiem podjęcia wzajemnych konsultacji za pośrednictwem EWRS i w ramach KBZ, za każdym razem w porozumieniu z Komisją, przede wszystkim odnośnie do środków zdrowia publicznego przyjętych lub które państwa zamierzają przyjąć w reakcji na zagrożenie, gdy poziom aktywacji EWRS wynosi 2 lub 3[57]. Następuje to na wniosek państwa lub Komisji i obejmuje zakresem wszelkie informacje, które uzyskano w ramach EWRS i oceny ryzyka przeprowadzonej przez uprawnione organy, np. ECDC. Celem konsultacji jest koordynacja reagowania krajowego i unijnego na poważne transgraniczne zagrożenia dla zdrowia, także wtedy gdy reakcja krajowa wynika równolegle z Międzynarodowych Przepisów Zdrowotnych i działań ŚOZ; oraz koordynacja wszelkiej komunikacji w zakresie ryzyka i występującej sytuacji kryzysowej. Taka horyzontalna komunikacja na poziomie uprawnionych organów UE i krajowych ma także zapewnić, że informacje dostarczane do pacjentów i służby zdrowia będą spójne i skoordynowane. Wreszcie, państwo członkowskie, które zamierza podjąć środki ochrony zdrowia publicznego w celu zwalczania zagrożenia, ma obowiązek powiadomić inne państwa i Komisję oraz przeprowadzić konsultacje „w sprawie charakteru celu i zakresu stosowania danych środków"[58].

[54] Art. 10 ust. 1 rozporządzenia 851/2004; Sprawozdanie 2015, s. 9.

[55] Por. też S. Kittelsen, *Conceptualizing Biorisk: Dread Risk and the Threat of Bioterrorism in Europe*, „*Security Dialogue*" 40, 2009, nr 1, s. 51–71.

[56] Art. 7 ust. 1–2 decyzji 1082/2013.

[57] Por. Załacznik II decyzji 200/57 ze zm.

[58] Art. 11 ust. 1–3 decyzji 1082/2013.

Podobne obowiązki i konsultacje występują *ex post*, gdy środki ochrony zdrowia zostały przyjęte w trybie pilnym, bez możliwości wcześniejszej konsultacji[59]. W efekcie występuje tutaj horyzontalne zarządzanie ryzykiem w ramach siatki powiązań (tzw. *network governance*) — typowe rozwiązanie dla unijnej polityki ochrony zdrowia, bezpieczeństwa produktów czy regulacji ryzyka w innym sektorze[60]. Dobrym przykładem działania systemu jest opis koordynacji reagowania zastosowany przez instytucje i państwa UE podczas epidemii Ebola.

> W odniesieniu do ogniska gorączki krwotocznej Ebola ze względu na wielosektorowy charakter tej choroby oprócz KBZ uruchomiono jednocześnie szereg innych narzędzi, w tym unijny mechanizm ochrony ludności (na wstępny wniosek WHO). Międzysektorową koordynację na szczeblu Unii ułatwiono również poprzez posiedzenia grupy zadaniowej ds. Eboli zorganizowane w Centrum Koordynacji Reagowania Kryzysowego Komisji. KBZ był użyteczny pod względem udziału w posiedzeniach tej grupy zadaniowej i przekazywania ich rezultatów organom ds. zdrowia publicznego. Ten wielopłaszczyznowy proces koordynacji wspomógł również utworzenie i funkcjonowanie unijnego systemu ewakuacji medycznej do Europy osób, u których stwierdzono lub podejrzewano gorączkę krwotoczną Ebola. […], natomiast funkcja „komunikacji selektywnej" w EWRS umożliwiła koordynację odpowiednich możliwości leczenia szpitalnego[61].

W kontekście niniejszych rozważań należy przyjąć, że również uruchomienie unijnej procedury ustalania kontaktów zakaźnych przez EWRS, tym bardziej, gdy ma ona objąć więcej państw członkowskich, wymaga konsultacji i skoordynowania na forum KBZ[62]. Treść decyzji wskazuje, że nawet uruchomienie wyłącznie krajowej procedury ustalania kontaktów zakaźnych (jeżeli dane państwo posiada odrębną procedurę) wymaga przekazania informacji do pozostałych państw członkowskich, jeżeli występuje poważne transgraniczne zagrożenie zdrowia. Obowiązek wymiany informacji obejmuje zatem niezwłoczne przekazanie za pośrednictwem EWRS wszelkich dostępnych informacji koniecznych do koordynacji reagowania, w tym danych osobowych, które są niezbędne do ustalenia kontaktów zakaźnych[63]. Może wystąpić więc sytuacja, że państwo członkowskie wdraża procedurę ustalania kontaktów zakaźnych przez EWRS równoległe z poinformowaniem o zagrożeniu, ponieważ np. poszukuje źródła zakażenia lub przekazuje informacje o źródle, tak aby zainteresowane państwa mogły ustalić i powiadomić osoby, które miały kontakt z tym źródłem zakażenia. Przy tym przekazywanie obowiązkowych

---

[59] Art. 11 ust. 3 decyzji 1082/2013. Zob. też decyzję 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności, Dz. Urz. UE 2013, L 347/924.

[60] Por. P. Dąbrowska-Kłosińska, *EU Governance of GMOs: Political Struggles and Experimentalist Solutions?*, [w:] *Experimentalist Governance in the European Union: Towards a New Architecture*, red. C.F. Sabel, J. Zeitlin, Oxford 2010, s. 177–210.

[61] Sprawozdanie 2015, s. 9–10.

[62] Art. 17 decyzji 1082/2013. Zob. też Commission Staff Working Document, *Health Security in the European Union and Internationally*, SEC(2009) 1622final oraz stronę Komisji poświęconą KBZ http://ec.europa.eu/health/preparedness_response/risk_management/index_en.htm (dostęp: 21.10.2016).

[63] Art. 9 ust. 3 i) decyzji 1082/2013.

informacji w ramach EWRS następuje przez dwa kanały, które obejmuje system. Pierwszy to tzw. kanał informacji ogólnej — umożliwia właściwemu organowi ds. zdrowia w danym państwie członkowskim przekazanie wszystkim krajowym punktom kontaktowym EWRS, Komisji, ECDC oraz WHO informacji o przypadkach spowodowanych poważnymi, transgranicznymi zagrożeniami podlegającymi obowiązkowi zgłaszania (wspomniane trzy poziomy zagrożeń, patrz punkt 4.3. *in fine*). Drugi to tzw. kanał informacji selektywnej — używany jest do wymiany informacji lub danych jeśli obejmują dane osobowe w ramach zastosowanych środków procedury ustalania kontaktów zakaźnych. Dotyczy zatem komunikowania się wyłącznie między tymi państwami członkowskimi, których dotyczy wymiana, i został stworzony specjalnie jako środek zabezpieczający w celu zagwarantowania i realizowania ochrony tajemnicy tych danych[64].

4.4.4. USTALANIE KONTAKTÓW ZAKAŹNYCH

Według definicji legalnej, którą zawiera decyzja 1082/2013, „ustalanie kontaktów zakaźnych" (tzw. *contact-tracing*, *la recherche des contacts*, *Ermittlung von Kontaktpersonen*) oznacza: „środki stosowane w celu wykrycia osób, które były narażone na działanie źródła poważnego transgranicznego zagrożenia zdrowia i u których występuje zagrożenie rozwinięcia się choroby lub u których ta choroba się rozwinęła"[65].

Procedura ta obejmuje więc środki ochrony zdrowia publicznego polegające na wydaniu decyzji ustalania „kontaktów zakaźnych" lub podjęciu szczególnych działań kontrolnych w celu identyfikacji zakażonych osób i osób narażonych na działanie źródła zagrożenia[66]. Przykładowo środki takie zostały podjęte w przypadku opisanego wyżej pana Andrew Speaker'a po jego podróży po Europie. W efekcie taka skoordynowana współpraca zainteresowanych państw członkowskich może wymagać wymiany za pośrednictwem systemu EWRS danych osobowych, w tym chronionych danych związanych ze zdrowiem i informacji o potwierdzonych lub podejrzewanych zakażeniach osób, które są poszukiwane. Wynika z tego, że wymiana informacji w celu ustalenia kontaktów przez EWRS obejmuje dane osobowe jednostek chronione zgodnie z unijnym ustawodawstwem, w tym dane medyczne, które należą do kategorii danych szczególnie chronionych[67]. Wymiany danych osobowych dokonują wyłącznie państwa członkowskie bezpośrednio zainteresowane środkami ustalania kontaktów zakaźnych, ponieważ np. na ich terytorium odbywała się podróż, start samolotu z lotniska itp. Komisja

---

[64] Por. Zalecenie Komisji nr 2012/73/UE w sprawie wytycznych w zakresie ochrony danych odnośnie do systemu wczesnego ostrzegania i reagowania (EWRS), Dz. Urz. UE 2012 L 36/31, pkt 5 (dalej: Zalecenie Komisji 2012/73).

[65] Art. 3 c) decyzji. Zob. też art. 2a, decyzji 2000/57.

[66] Art. 3 f) decyzji 1082/2013. Zob. też punkty 25–27 preambuły, decyzja 1082/2013.

[67] *Podręcznik europejskiego prawa…*, s. 44. Zob. też sprawy C-101/01 *Bodil Lindqvist*, F-46/09 *V przeciwko Parlamentowi Europejskiemu*, *op. cit.*

jest zawsze powiadamiana w sytuacji użycia modułu selektywnego, ale co do zasady nie bierze udziału w wymianie danych osobowych. Włączenie Komisji może nastąpić, jeśli wyjątkowe okoliczności wymagałyby tego do koordynacji działań lub umożliwienia szybkiego i skutecznego wprowadzenia środków ochrony zdrowia publicznego[68].

Decyzja 1082/2013 reguluje proces przekazywania danych osobowych: musi odbywać się on za pośrednictwem tzw. „selektywnego modułu przekazywania wiadomości", który, jak wyżej wspomniano, umożliwia transfer danych osobowych wyłącznie do właściwych organów krajowych, które zajmują się środkami ustalania kontaktów zakaźnych. Decyzja jednak nie precyzuje, jakie konkretnie dane osobowe podlegać mogą przekazywaniu, ograniczając się do wskazania, że ostrzeżenie z art. 9 decyzji może zawierać informacje takie jak „dane osobowe niezbędne w celu ustalenia kontaktów zakaźnych"[69].

Zakres przedmiotowy danych osobowych (zob. Tabela 1), które mogą być przekazane, uregulowany został w przepisach wykonawczych (załącznik III, decyzja 2000/57). Przepisy te, które zostały wydane pod rządami aktu obowiązującego poprzednio (decyzji 2119/98/WE), nie zostały na razie uaktualnione i dostosowane np. do rozszerzonego zakresu przedmiotowego całej decyzji 1082/2013[70]. Warto też zauważyć, że tłumaczenie polskie przedmiotowego załącznika wskazuje, iż „wykaz danych na potrzeby ustalania kontaktów zakaźnych" to lista zamknięta, tłumaczenia zaś w innych językach urzędowych jednoznacznie wskazują, że jest to lista przykładowa (*indicative list*, *als Hinweis dinende Aufstellung*, *Liste indicative*, *Elenco indicativo*). Biorąc pod uwagę bardzo szeroki zakres informacji, które mogą być ujawnione, oraz cel zapewnienia efektywnej ochrony danych osobowych, można stwierdzić, że jest to istotna kwestia interpretacyjna. Komisja zaleca rozumienie wąskie, zastrzegając, że upoważnienia do przekazywania określonego rodzaju danych wymienionych we wspomnianym załączniku nie należy traktować jako upoważnienia blankietowego oraz że rozszerzenie wskazanego tam zakresu danych (Tabela 1) oznaczałoby najpewniej naruszenie zasady proporcjonalności. Komisja wskazuje, że:

> Wykazu danych osobowych, które można przekazywać na potrzeby ustalania kontaktów zakaźnych, znajdującego się w załączniku […], nie można traktować jako generalnego i bezwarunkowego upoważnienia do przetwarzania tych kategorii danych. Jednocześnie należy zachować najwyższą ostrożność przy przetwarzaniu danych osobowych innych niż te wymienione we wspomnianym załączniku, gdyż ich ujawnienie byłoby najprawdopodobniej niepotrzebne i niezasadne.

---

[68] Sprawozdanie 2007, s. 8; Zalecenie Komisji 2012/73, *op. cit.*, pkt 5.

[69] Art. 9 ust. 3 i) w związku z art. 16 ust. 2 decyzji 1082/2013.

[70] Załącznik I, decyzja Komisji 2000/57/WE w sprawie systemu wczesnego ostrzegania i reagowania w celu zapobiegania i kontroli chorób zakaźnych na mocy decyzji nr 2119/98/WE Parlamentu Europejskiego i Rady, ze zmianami, Dz. Urz. WE 2000 L 21/32; tekst jednolity, nr CELEX 2000D0057-PL-14.07.2009-002.001-2.

Organ krajowy powinien każdorazowo przy wysyłaniu wiadomości zawierającej dane osobowe systemem selektywnego kanału komunikacji dokonać oceny poszczególnych przypadków (czyli tzw. *case-by-case basis*) pod kątem zakresu przedmiotowego danych i udostępniać tylko te, które są „absolutnie konieczne" do przeprowadzenia skutecznej procedury ustalania kontaktów zakaźnych[71].

Tabela 1. Procedura ustalania kontaktów zakaźnych — lista danych osobowych

Przykładowy wykaz danych osobowych na potrzeby ustalania kontaktów zakaźnych	
1. Informacje osobowe	— Nazwisko i imiona; — Narodowość, data urodzenia, płeć; — Typ dokumentu tożsamości, numer dokumentu i organ wydający; — Aktualny adres zamieszkania (ulica i numer domu, miasto, państwo, kod poczt.); — Numery telefonów (komórkowego, stacjonarnego, służbowego); — Adres e-mail (prywatny, służbowy).
2. Informacje na temat podróży	— Dane dotyczące środka podróży (np. numer lotu, data lotu, nazwa statku, numery rejestracyjne pojazdu); — numer(-y) miejsc(-a); — numer(-y) kabin(-y).
3. Informacje umożliwiające kontakt	— Nazwiska odwiedzonych osób/nazwy miejsc pobytu; — Daty pobytu i adresy miejsc pobytu (ulica i numer domu, miasto, państwo, kod pocztowy); — Numery telefonów (komórkowego, stacjonarnego, służbowego); — Adres e-mail (prywatny, służbowy).
4. Informacje dotyczące osób towarzyszących	— Nazwisko i imiona; — Narodowość; — Informacje osobowe zgodnie z pkt 1, tiret trzecie do szóstego.
5. Dane osoby, którą należy powiadomić w razie wypadku	— Nazwisko osoby, którą należy powiadomić; — Adres (ulica i numer domu, miasto, państwo, kod pocztowy); — Numery telefonów (komórkowego, stacjonarnego, służbowego); — Adres e-mail (prywatny, służbowy).

Źródło: opracowanie na podstawie Załącznik III, decyzja 2000/57/WE.

W celu lepszego zobrazowania działania systemu EWRS i procedury ustalania kontaktów zakaźnych warto przytoczyć przykłady przedstwiona w sprawozdaniu Komisji z 2007 r. opisującym działanie EWRS w 2004 roku[72]. W trakcie tego roku przez kanały EWRS zostało wysłanych 105 ostrzeżeń i 157 komentarzy właściwych organów krajowych ds. ochrony zdrowia, z których 9 spowodowało konieczność skoordynowanej reakcji na poziomie UE i do nich w większości od-

[71] Por. Zalecenie Komisji 2012/73, pkt 6.

[72] Sprawozdanie 2007, s. 5–6. Zob. też przykłady w Report on the Operation of the Early Warning and Response System of the Community Network for the Epidemiological Surveillance and Control of Communicable Diseases (Decision 2000/57/EC) during 2002 and 2003, COM(2005) 104 final (dalej: Sprawozdanie 2005).

nosiły się komentarze (126/157). Dla porównania w 2006 roku miały miejsce 138 zgłoszenia i 223 komentarze; a w latach 2013–2015 odpowiednio 168 wiadomości i 354 komentarze do nich[73].

Z punktu widzenia ochrony danych i uruchomienia procedury ustalania kontaktów można przytoczyć następujące przykłady: dwa przypadki dotyczyły choroby legionistów (Legionelloza, rodzaj ciężkiego zapalenia płuc) i gorączki Pontiac. Zgłoszone zostały przez Niemcy i Włochy — oba przypadki były związane z podróżami turystów statkami wycieczkowymi i wymagały ustalenia kontaktów, tj. wszystkich osób, które były narażone na kontakt ze źródłem zakażenia, oraz zaalarmowania właściwych organów zdrowia publicznego państw członkowskich, aby podjęły odpowiednie środki w portach docelowych. Jeden przypadek dotyczył gorączki Zachodniego Nilu turysty irlandzkiego, który zaraził się podczas wakacji w Portugalii i był następnie monitorowany przez oba państwa. Nadto został zgłoszony przypadek wściekłego psa, nielegalnie wwiezionego do Unii, który miał kontakt z wieloma osobami i dziećmi w kilku turystycznych regionach Francji — zastosowanie procedury EWRS i ustalenia kontaktów pozwoliło na szybkie powiadomienie i zaszczepienie tych osób[74]. Wreszcie, jeden przypadek doprowadził do poszukiwania pasażerów samolotu, którzy mieli/mogli mieć kontakt z pasażerem-turystą przemycającym do UE w bagażu podręcznym dwa ptaki drapieżne z Tajlandii zainfekowane wirusem ptasiej grypy A/H5N1, a które zostały zatrzymane przez kontrolerów na lotnisku *Zaventem* w Belgii[75]. Podobna sytuacja miała miejsce w 2007 roku, gdy zidentyfikowano i skontaktowano się z prawie 284 turystami z jedenastu krajów UE, którzy przebywali na wakacjach w jednym z tajlandzkich hoteli, ponieważ u kilku gości zdiagnozowano Legionellozę[76].

Trzeba na koniec zaznaczyć, że decyzja o wdrożeniu środków ustalania kontaktów przez jedno lub więcej państw UE nie musi każdorazowo oznaczać przekazywania danych osobowych przez elektroniczny system EWRS, choć jest to możliwe pod warunkiem spełnienia wymaganych przesłanek (patrz niżej). Może to też nastąpić w formie faktycznej podczas spotkań KBZ na szczeblu UE. Za każdym razem kluczowe jest, aby przy całym stosowaniu decyzji 1082/2013, w szczególności przy stosowaniu środków ustalania kontaktów, w pełni respektowano europejskie prawo ochrony danych osobowych. Decyzja 10082/2013 zawiera szczególne postanowienia, a system EWRS został wyposażony w specjalne mechanizmy zapewniające skuteczność ochrony danych osobowych. Ich celem jest efektywne wdrożenie ochrony prawnej jednostek ustanowionej na poziomie UE za pośrednictwem przepisów horyzontalnych, np. dyrektywy 95/46. Kwestie te zostaną przedstawione poniżej.

---

[73] Sprawozdanie 2009, s. 3; Sprawozdanie 2015, s. 9.

[74] Por. także F. Bombillar, *The Case of Pandemic Flu Vaccines: Some Lessons Learned*, „European Journal of Risk Regulation" 1 (4), 2010, s. 427–431.

[75] Sprawozdanie 2007, s. 6.

[76] Sprawozdanie 2009, s. 6.

5. OCHRONA DANYCH OSOBOWYCH PRZY UNIJNYM PRZECIWDZIAŁANIU ZAGROŻENIOM DLA ZDROWIA PUBLICZNEGO

Dotychczasowe rozważania analizujące system wzajemnego komunikowania się państw członkowskich i instytucji UE w sytuacji kryzysowej poważnego zagrożenia dla zdrowia pokazały, że kwestia ochrony danych osobowych jednostek, których osobiście może dotyczyć sytuacja, jest bardzo istotna i może mieć znaczenie praktyczne. Dzieje się tak przede wszystkim z powodu zakresu przedmiotowego i wrażliwości danych, które mogą zostać przekazane (nie tylko dane osobowe, lecz także dane medyczne), jak również potencjalnej ilości zaangażowanych organów różnych państw członkowskich i skali działań.

Rozwój przepisów i rozwiązań instytucjonalnych realizujących ochronę danych osobowych w kontekście ochrony zdrowia publicznego na poziomie UE następował stopniowo i częściowo równolegle do rozwoju narzędzi komunikacji między właściwymi organami ds. zdrowia, które te dane mogły wymieniać. Obecny system jest więc wynikiem dwóch poniekąd współzależnych trendów legislacyjnych w UE. Pierwszy oznaczał stopniowe wzmacnianie prawa do ochrony danych osobowych w UE w ogóle przy udziale władzy legislacyjnej oraz orzecznictwa i w szczególności w kontekście zagrożeń dla zdrowia[77]. Drugi obejmuje rozwój integracji i regulacji w obszarze ochrony zdrowia publicznego z uwzględnieniem konieczności zapewnienia ochrony danych osobowych.

Początkowo przepisy regulujące działanie EWRS ustanowionego w decyzji 2119/98/WE i odpowiednich przepisach wykonawczych (decyzja 2000/57/WE) nie zawierały rozwiązań szczególnych służących ochronie danych osobowych, które jednak były chronione na mocy zasad ogólnych i wyjątków wynikających z dyrektywy 95/46/WE (mającej zastosowanie także do obecnego systemu). W miarę upływu czasu, a także rozwoju technologicznego oraz rozwoju ryzyka globalnych niebezpieczeństw dla zdrowia i przepisów międzynarodowych będących reakcją na te zagrożenia (Międzynarodowe Przepisy Zdrowotne weszły w życie w 2007 roku), pojawiła się jednak potrzeba ustanowienia szczególnych gwarancji ochrony danych w przypadku wymiany danych osobowych i medycznych między państwami członkowskimi w trakcie procedury ustalania kontaktów zakaźnych. W efekcie w marcu 2005 uruchomiono w ramach EWRS wspomniany kanał komunikacji selektywnej (patrz wyżej), a w 2009 roku w przepisach wykonawczych dodano specjalny artykuł nakładający dodatkowe wymagania na właściwe organy celem specjalnego zabezpieczenia i zwiększenia efektywności ochrony danych przy uruchomianiu tej procedury[78]. Wreszcie, cały system chroniący wymianę

[77] Zob. rozporządzenie 2016/679; por. też wyroki TSUE, np. C-131/12 Google Spain.

[78] Por. art. 2a decyzji 2000/57 dodany na mocy decyzji 2009/547, Commission Decision 2009/547/EC of 10 July 2009 amending Decision 2000/57/EC on early warning and response sys-

danych osobowych w ramach EWRS i obowiązujące zabezpieczenia zostały przedstawione przez Komisję do oceny Europejskiemu Inspektorowi Ochrony Danych („EIOD"), który w ramach tzw. kontroli wstępnej wydał opinię wskazującą liczne niedociągnięcia w tych przepisach i mnóstwo możliwych zagrożeń dla praw podstawowych wynikających z przetwarzania na większą skalę danych dotyczących ustalania kontaktów zakaźnych w przypadku wystąpienia w przyszłości poważnych zagrożeń dla zdrowia związanych z pandemią[79]. W efekcie Komisja w 2012 roku wydała szerokie wytyczne dla użytkowników systemu EWRS, w tym krajowych organów odpowiedzialnych za przekazywanie informacji do systemu, w celu uwzględnienia zaleceń EIOD oraz pomocy w jaśniejszym określeniu odpowiednich ról, zadań i obowiązków różnych podmiotów systemu i zagwarantowania w ten sposób skutecznego przestrzegania przepisów o ochronie danych[80]. Następnie projekt obecnie obowiązującej decyzji 1082/2013 o poważnych transgranicznych zagrożeniach dla zdrowia był także przedmiotem opinii Europejskiego Inspektora Ochrony Danych na etapie procedury legislacyjnej[81].

W rezultacie obecny system ustanawia przepisy zabezpieczające wysoki poziom ochrony danych osobowych przy założeniu, że przestrzegane są zarówno przepisy horyzontalne UE o ochronie danych osobowych i KPP, jak i obowiązujące regulacje dotyczące ochrony zdrowia publicznego wynikające z decyzji 1082/2013 oraz przepisów wykonawczych (przede wszystkim zmieniona w 2009 roku decyzja 2000/57/WE) i wytycznych Komisji (Zalecenie 2012/73/UE).

Obowiązujące gwarancje szczególne ochrony danych osobowych w kontekście procedury ustalania kontaktów zakaźnych w ramach przeciwdziałania transgranicznym zagrożeniom dla zdrowia zostaną przedstawione poniżej. Tekst koncentruje się na tej procedurze, ponieważ zgodnie z decyzją 1082/2013 powiadomienie o zagrożeniu z art. 9 może zawierać dane osobowe tylko wtedy, gdy są one „niezbędne w celu ustalenia kontaktów zakaźnych, zgodnie z art. 16" decyzji. Tekst decyzji, a więc aktu prawnego regulującego istotne elementy w świetle art. 291 TFUE, ustala zatem od razu konkretny cel przekazywania danych osobowych — ma to być identyfikacja osób narażonych na zagrożenie zdrowotne lub już

---

tem for the prevention and control of communicable diseases under Decision No 2119/98/EC of the European Parliament and of the Council, OJ 2009 L 181/57.

[79] Por. pkt 6 preambuły do Opinii o kontroli wstępnej z dnia 26 kwietnia 2010 r. wydanej przez Europejskiego Inspektora Ochrony Danych w odniesieniu do systemu wczesnego ostrzegania i reagowania, notyfikowanego przez Komisję Europejską w dniu 18 lutego 2009 r. (sprawa C 2009-0137). Opinia ta została opublikowana na stronie internetowej Europejskiego Inspektora Ochrony Danych pod następującym adresem: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/ Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_EN.pdf (dostęp: 20.10.2016).

[80] Zalecenie Komisji nr 2012/73.

[81] Opinia EIOD, 28.03.2012.

dotkniętych tym zagrożeniem oraz nakaz respektowania zasady proporcjonalności — dane osobowe maja być niezbędne do realizacji celu[82].

5.1. KLAUZULA OCHRONY DANYCH OSOBOWYCH Z ART. 16 DECYZJI 1082/2013

Należy powtórzyć, że zasadniczo system EWRS nie służy przekazywaniu danych osobowych, a raczej wzajemnemu informowaniu państw członkowskich o nowych zjawiskach epidemiologicznych, chorobach, innych zagrożeniach czy zastosowanych lub sugerowanych środkach kontroli. Wymiana danych osobowych nastąpi tylko wtedy, gdy w ramach ustalania kontaktów zakaźnych komunikowane są dane osób fizycznych, w tym dane szczególnie chronione dotyczące zdrowia.

Kluczowym przepisem dotyczącym ochrony danych osobowych przy przeciwdziałaniu transgranicznym poważnym zagrożeniom dla zdrowia jest art. 16 decyzji 1082/2013, który wprowadza dodatkowe gwarancje ochrony w tym kontekście. Klauzula, mimo że stanowi swoisty *lex specialis* do przepisów ogólnych ochrony danych w UE, tj. dyrektywy 95/46 i rozporządzenia 2001/45, jednocześnie odsyła do tych aktów i uszczegóławia je[83]. Tym samym przy wszelkim przetwarzaniu danych na podstawie decyzji 1082/2013 muszą być respektowane unormowania obu tych aktów prawnych, a od 25 maja roku 2018 — rozporządzenia 2016/679. W szczególności chodzi o zasady ogólne dotyczące: legalności przetwarzania danych i ograniczania go co do celów, a więc zgodności z zasadą proporcjonalności; jakości danych; zachowywania danych i udzielania dostępu podmiotom danych, oraz innych praw przysługujących podmiotom danych; a także dotyczące poufności i bezpieczeństwa danych. W konsekwencji do oceny legalności i uzasadnienia przetwarzania danych w ramach EWRS będą miały zastosowanie kryteria i jasno sprecyzowane warunki z art. 7 i 8 dyrektywy 95/46 (zob. punkt 2 powyżej i 6.2. niżej)[84].

W art. 16 decyzji 1082/2013 znajdują się także konkretne obowiązki dla organów krajowych, które są uznawane za administratorów danych w rozumieniu dyrektywy 95/46, o ile pełnią obowiązki w zakresie wysyłania ostrzeżeń i prostowania danych osobowych w systemie EWRS. W odniesieniu do przechowywania danych osobowych administratorem danych jest też Komisja[85]. Po pierwsze

---

[82] W tekście pomijam kwestie przetwarzania danych osobowych użytkowników sieci EWRS, np. ich danych kontaktowych, ponieważ jest to nierozerwalnie związane ze skutecznym realizowaniem zadań przez EWRS i jego obsługą, jest objęte ogólnymi regułami prawa UE dla ochrony danych i występuje też w innych kontekstach prawa unijnego, a zatem nie jest wyjątkowe i szczególne dla przypadków omawianych w niniejszym tekście.

[83] W niniejszym tekście odnoszę się głownie do przepisów obowiązującej dyrektywy 95/46 o ochronie danych, skierowanej do państw członkowskich UE. Należy jednak przyjąć, że rozporządzenie 2001/45 skierowane do organów i instytucji UE zawiera co do zasady analogiczne postanowienia.

[84] Por. Zalecenie Komisji nr 2012/73, pkt 4.

[85] Art. 16 ust. 1 i 7–8, decyzja 1082/2013. Zob. art. 20 ust. 4, rozporządzenie 851/2004, w odniesieniu do ECDC.

państwa członkowskie i ich organy oraz Komisja i instytucje UE powinny podjąć wszelkie „odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą lub nieuprawnionym dostępem oraz przed wszelką formą nielegalnego przetwarzania”[86]. Następnie, jeśli organy krajowe wdrażają środki i procedurę ustalania kontaktów zakaźnych i w tym celu przekazują dane osobowe, są zobowiązane: (i) do używania wyłącznie selektywnego modułu przekazywania wiadomości wbudowanego w EWRS; (ii) przekazywania wiadomości wyłącznie państwom członkowskim zainteresowanym tymi środkami; (iii) odniesienia się do ostrzeżenia z art. 9 decyzji 1082/2013 przekazanego uprzednio za pośrednictwem kanału ogólnego EWRS; (iv) natychmiastowego poinformowania wszystkich zainteresowanych państw, jeśli organ stwierdził, że przekazanie danych było sprzeczne z dyrektywą 95/46, ponieważ przekazanie danych nie było konieczne do celów wdrożenia procedury — czyli przy wdrażaniu środków ustalania kontaktów zakaźnych została naruszona zasada proporcjonalności[87].

Budowa operacyjna platformy EWRS jest także efektem regulacji art. 16 decyzji 1082/2013. Poza obowiązkowym modułem selektywnego przekazywania wiadomości umożliwiającym przekazywanie danych osobowych wyłącznie do właściwych organów krajowych, które zajmują się środkami ustalania kontaktów zakaźnych, EWRS musi zawierać wiele zabezpieczeń służących temu, aby dane osobowe dotarły wyłącznie do organów, które tego potrzebują, i aby każdorazowo przy wejściu do systemu organy oceniały dane pod kątem ich ochrony i zastosowania zasady proporcjonalności[88]. Konkretne zabezpieczenia wbudowane w EWRS polegają na:

— ograniczonym dostępie do EWRS tylko dla uprawnionych organów krajowych ds. zdrowia wyznaczonych przez państwa członkowskie;

— specjalnym ostrzeżeniu zamieszczonym na stronie EWRS, że kanał informacji ogólnej nie służy do przekazywania danych osobowych i uruchamiania procedury ustalania kontaktów zakaźnych;

— domyślnym wyłączeniu w systemie za pośrednictwem specjalnej opcji wyłączającej udział Komisji i ECDC z tej procedury z listy odbiorców danych przesyłanych w kanale dystrybucji selektywnej (opcja ta może tylko wyjątkowo być włączona, jeśli wymaga tego zagrożenie);

— posiadaniu specjalnej funkcji pozwalającej użytkownikom bezpośrednio korygować lub usuwać w dowolnym czasie te wysyłane selektywnie wiadomości, zawierające dane osobowe, które są nieprecyzyjne, nieaktualne, już niepotrzebne lub w jakikolwiek inny sposób niezgodne z wymogami w zakresie ochrony danych;

---

[86] Art. 16 ust. 1, decyzja 1082/2013.

[87] Art. 16, decyzja 1082/2013. Zob. Zalecenie Komisji 2012/73/WE, pkt 7 i 9 oraz Opinia EIOD, 26.04.2010.

[88] Art. 16 ust. 1–3 i 5–6, decyzja 1082/2013; oraz Zalecenie Komisji 2012/73/WE, pkt 7.

— posiadaniu specjalnej funkcji usuwania wszystkich selektywnie wysłanych wiadomości zawierających dane osobowe 12 miesięcy od daty wysłania wiadomości;

— i wreszcie, co jest szczególnie istotne dla egzekwowania praw podmiotów danych i odpowiedzialności administratorów za ich naruszenie, specjalnym mechanizmie umożliwiającym organom krajowym, których dotyczy dana procedura, ustalanie kontaktów i wymianę informacji, komunikację i współpracę w zakresie dostępu, korekty, zablokowania lub usunięcia wniosków podmiotów danych[89].

5.2. USTALANIE KONTAKTÓW ZAKAŹNYCH A WARUNKI LEGALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH W ŚWIETLE DYREKTYWY 95/46 I ROZPORZĄDZENIA 2016/679

Podstawowymi kwestiami, które wymagają omówienia w kontekście funkcjonowania EWRS i przekazywania danych osobowych w ramach wdrażania procedury ustalania kontaktów zakaźnych, są, po pierwsze, warunki legalności przetwarzania danych osobowych, w tym danych szczególnie wrażliwych dotyczących zdrowia, przy stosowaniu decyzji 1082/2013 przez organy krajowe i UE. Założenie spełnienia tych warunków oznacza, że przekazywanie danych jest zgodne z prawem, ponieważ mieści się to w ramach przewidzianych wyjątków, mimo np. niemożności uzyskania zgody podmiotu danych. W szczególności może to nastąpić w sytuacji braku wyrażenia zgody przez podmiot danych z powodów o charakterze subiektywnym (np. stan zdrowia) lub obiektywnym (np. podmiot danych nie wie, że miał kontakt ze źródłem zakażenia). Po drugie prawa podmiotów danych i odpowiednio odpowiedzialność właściwych organów, gdy mimo przewidzianych zabezpieczeń i zobowiązań dla organów doszło np. do bezprawnego udostępnienia danych.

Trzeba wskazać, że prawem właściwym do oceny zgodności działań w ramach EWRS z zasadami ochrony danych osobowych czy kwestii np. udzielenia zgody będzie prawo krajowe, w tym ustawodawstwo transponujące dyrektywę 95/46[90]. Warto też podkreślić, iż dyrektywa o ochronie danych osobowych, mimo ustanowienia harmonizacji całkowitej, pozostawia państwom członkowskim możliwość wprowadzania w określonych przypadkach wyjątków lub odstępstw od niektórych przepisów. Komisja wyjaśnia, że: „w krajowych przepisach o ochronie danych, którym podlega użytkownik EWRS, mogą być określone surowsze wymogi dotyczące ochrony danych lub wymogi specyficzne dla danego kraju, nieprzewidziane w aktach prawnych innych państw członkowskich”[91]. Przepisy krajowe różnić się mogą także w odniesieniu do wymogów dotyczących przetwarzania kategorii danych osobowych dotyczących zdrowia osób fizycznych, dlatego Komisja zaleca

[89] Art. 16, decyzja 1082/2013; Zalecenie Komisji 2012/73/WE, pkt 7.

[90] Zob. *Podręcznik europejskiego prawa …*, s. 18; oraz Zalecenie Komisji nr 2012/73, pkt 3.

[91] *Ibidem.*

państwom pogłębioną współpracę między organami ochrony zdrowia i właściwymi organami krajowymi ochrony danych osobowych[92].

W świetle dyrektywy 95/46/WE wszelkie przetwarzanie danych osobowych w EWRS musi być uzasadnione określonymi podstawami prawnymi, które istnieją dzięki decyzji 1082/2013 i stosownym przepisom wykonawczym. Ponadto do oceny legalności wymiany w EWRS danych osobowych dotyczących kontaktów zakaźnych osób fizycznych (np. danych kontaktowych osób zakażonych, danych dotyczących środka podróży i innych danych związanych z trasą podróży oraz miejscami pobytu danej osoby, informacji o odwiedzonych osobach i osobach potencjalnie narażonych na zakażenie) mogą mieć zastosowanie następujące kryteria[93]: po pierwsze — wykonanie zobowiązania prawnego administratora danych wynikającego z decyzji 1082/2013; po drugie — ochrona żywotnych interesów osób, których dane dotyczą. Oznacza to, że wymiana między zainteresowanymi państwami członkowskimi danych osobowych osób zakażonych, a także osób bezpośrednio zagrożonych zakażeniem, może być konieczna do zapewnienia im odpowiedniej opieki lub leczenia, z uwagi na ochronę zdrowia tych osób i obywateli UE w ogóle; po trzecie — kryterium tzw. interesu publicznego. Należy rozumieć, że cały system EWRS ma służyć wykonywaniu leżących w interesie publicznym zadań, które zostały powierzone państwom członkowskim w celu ochrony zdrowia publicznego i kontroli zapobiegania poważnym transgranicznym zagrożeniom dla zdrowia publicznego[94].

Szczególnej ocenie będzie podlegać sytuacja, w której wymiana danych osobowych obejmie także dane dotyczące zdrowia. Wymiana danych szczególnie chronionych w ramach EWRS jest dozwolona na podstawie dyrektywy 95/46/WE tylko w bardzo ograniczonej liczbie przypadków[95]. Poza przypadkiem udzielenia zgody osoby zainteresowanej w omawianym kontekście najistotniejszy jest wyjątek z art. 8 ust. 3 (por. wyżej cytat w punkcie 2). Działanie EWRS zakłada możliwość istnienia konieczności szybkiej interwencji w wyjątkowych sytuacjach sanitarnych czy zagrożeń transgranicznych, gdy przekazanie podmiotowi danych wszystkich informacji, jakich potrzebuje, by móc wyrazić świadomą zgodę, jest niemożliwe. Może tez istnieć sytuacja, gdy w momencie gromadzenia danych niekoniecznie wiadomo, czy dane zostaną ostatecznie ujawnione za pośrednictwem systemu EWRS. Przy stosowaniu tego wyjątku ważne jest, aby uprawnione organy krajowe każdorazowo przeprowadziły odpowiedni proces decyzyjny, który wymaga oceny ryzyka i przeprowadzenia rachunku zysków i strat z punktu widzenia korzyści dla zdrowia publicznego z przekazywania danych dotyczących zdrowia odbiorcom z innych państw członkowskich. Decyzja w każdym poszczególnym przypadku powinna być podjęta na podstawie dostępnych dowodów naukowych

[92] *Ibidem.*

[93] Art. 7 lit. c), d) oraz e) dyrektywy 95/46/WE; Zalecenie Komisji nr 2012/73, pkt 4.

[94] *Ibidem.*

[95] Zob. art. 8 ust. 2, 3, 4 i 5 dyrektywy 95/46/WE.

w świetle oceny ryzyka organów państw członkowskich, a także ECDC i WHO. Jest to nieodzowne dla sprawdzenia, czy podjęte przekazanie danych osobowych jest „niezbędne i konieczne" dla celów ustalenia kontaktów, czyli respektowania zasady proporcjonalności[96]. Innymi słowy, właściwy organ wysyłający wiadomość powinien udostępnić organom z innego zainteresowanego państwa członkowskiego tylko te dane osobowe, które są konieczne do jednoznacznej identyfikacji osób zakażonych lub narażonych na zakażenie, i które zasadniczo nie wykraczają poza unijny wykaz (zob. Tabela 1 i wyjaśnienia w punkcie 4.4.4.).

Prawa dostępu podmiotów danych, ujawniania danych osobom trzecim przez administratorów oraz korekty danych i ustalenia ewentualnej odpowiedzialności w razie naruszeń będą także oceniane w świetle przepisów dyrektywy 95/46. Zalecenie Komisji 2012/73 zawiera też w tych kwestiach obszerne wyjaśnienia[97]. W szczególności — właściwy organ biorący udział w danej wymianie informacji nie może odmówić podmiotowi dostępu do danych ani ich korekty lub usunięcia, twierdząc, że to nie on wprowadził dane do systemu EWRS, lub że podmiot danych powinien zwrócić się do innego właściwego organu, ponieważ EWRS jest klasycznym przykładem wspólnej administracji. W szczególności, jeżeli wniosek podmiotu danych otrzyma niewłaściwy organ — inny niż ten, który wysłał pierwotne informacje poprzez kanał komunikacji selektywnej — organ otrzymujący wniosek powinien go przekazać za pomocą specjalnego mechanizmu wbudowanego w EWRS właściwemu organowi, który zamieścił pierwotne informacje, aby ten rozpatrzył wniosek[98].

5.3. ISTNIEJĄCE ZASTRZEŻENIA DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

Na koniec zostaną wskazane istniejące zastrzeżenia dotyczące efektywnego zapewniania ochrony danych osobowych w UE przy możliwym stosowaniu postanowień regulujących przeciwdziałanie poważnym zagrożeniom dla zdrowia o charakterze transgranicznym.

Podstawowym zarzutem wobec obecnego stanu prawnego jest brak dostosowania aktów wykonawczych do rozszerzonego zakresu przedmiotowego decyzji 1082/2013, ponieważ poprzednie działanie EWRS obejmowało tylko choroby zakaźne. Nie istnieją zaktualizowane przepisy wykonawcze i delegowane, np. do art. 6 ust. 5; art. 7 ust. 3; art. 8 ust. 2, art. 11 ust. 5, decyzji 1082/2013 — a zatem procedury działania i wdrażania EWRS czy przeprowadzania konsultacji i koordy-

[96] Por. art. 16 ust. 3 i 6, decyzja 1082/2013; art. 2a, decyzja 2000/57; i Zalecenie Komisji nr 2012/73, pkt 6. Dodatkowe przesłanki do przetwarzania danych dotyczących zdrowia mogą być także określone w odpowiednich krajowych aktach prawnych transponujących dyrektywę 95/46/WE lub w decyzji krajowych organów ochrony danych, zob. art. 8 ust. 4 dyrektywy 95/46/WE.

[97] Zalecenie Komisji nr 2012/73, pkt 6.

[98] *Ibidem*, pkt 9.

nacji wynikają częściowo z samej decyzji, a poza tym głównie z tekstu Załącznika II do decyzji 2000/57 czy Zalecenia Komisji 2012/73, a więc prawa miękkiego[99].

Wydanie przepisów wykonawczych pozwoliłoby na lepsze określenie jednolitych warunków wdrażania środków ustalania kontaktów zakaźnych i szczegółów tych działań, szczególnie przy potrzebie rozróżnienia zakażeń chorobowych i innych zagrożeń. Brak nowych, kompletnych przepisów wykonawczych powoduje też brak spójności między przepisami, które z reguły można sanować przez wykładnię, ale mogłoby mieć to wpływ na poziom ochrony danych osobowych, zwłaszcza gdyby wystąpiło zagrożenie zdrowia o charakterze masowym.

Przykładowo, nie ma formalnie spójności między art. 9 decyzji 1082/2013 a przepisami wykonawczymi z decyzji 2000/57, w szczególności art 2a, np. w odniesieniu do tego, które przypadki zagrożeń podlegają zgłoszeniu w ramach EWRS, i w konsekwencji — kiedy może się pojawić potrzeba ustalania kontaktów i przekazywania danych. Przepisy wcześniejsze (por. załącznik 1 decyzji 2000/57, ostatnio modyfikowany w 2009 roku, aby dostosować go do Międzynarodowych Przepisów Zdrowotnych) dotyczyły tylko chorób zakaźnych, a obecne dotyczą poważnych transgranicznych zagrożeń, w tym chorób (por. art. 9 w zw. z art. 2 decyzji 1082/2013). Istniejącą niespójność można sanować przez wykładnię systemową (przepisy nie są wprost sprzeczne, więc można założyć możliwość spójnej interpretacji), stosowanie reguł kolizyjnych (*lex posterior derogat legi priori*), oraz respektując hierarchię źródeł prawa UE (decyzja 1082/2013 jest aktem prawa wtórnego wydanego na podstawie TFUE, a więc wyższego rzędu niż decyzja wykonawcza Komisji 2000/57 wydana na podstawie decyzji), jednak — jak każda taka sytuacja w prawie — może to wpływać na efektywność stosowania i zapewniania ochrony[100]. Brak też spójności między szerszym zakresem przedmiotowym decyzji 1082/2013 a wyjątkiem z art. 8 ust. 3 dyrektywy 95/46, dlatego w razie zagrożenia dla zdrowia innego niż choroba zakaźna dopiero wejście w życie nowego rozporządzenia 2016/679 o ochronie danych roku sanuje tę sytuację. Z tekstu decyzji 1082/2013 nie wynika też jednoznacznie, że w ramach monitorowania doraźnego nie będą przekazywane dane osobowe, choć systematyka całej decyzji na to wskazuje[101].

Kilka kwestii może budzić dalsze wątpliwości z punktu widzenia zapewniania efektywnej ochrony danych osobowych. Dotyczy to możliwie jaśniejszego określenia sposobu realizowania odpowiedzialności właściwych organów, które miały dostęp do danych, szczególnie gdy nastąpiło bezprawne udostępnienie danych podczas ustalania kontaktów na poziomie UE. Stosowna informacja mogłaby znajdować się na stronie Komisji i/lub ECDC. Na stronie Komisji nie ma żadnej informacji o ochronie danych osobowych w kontekście transgranicznych zagrożeń,

[99] W chwili pisania niniejszego tekstu do decyzji 1082/2013 nie wydano jeszcze żadnych aktów wykonawczych ani delegowanych.

[100] Por. także konkluzje z opinii EIOD, 28.03.2012, dotyczące pozostałych zastrzeżeń.

[101] *Ibidem.*

jak wynika z deklaracji w wytycznych[102]. W ogólności np. strona internetowa ECDP jest mało przejrzysta i niezrozumiała, a także nie zawiera odniesień do relewantnych aktów prawnych. Natomiast informacje na stronie Dyrekcji Generalnej do Spraw Zdrowia są podzielone w 2 zakładkach: bezpieczeństwo przed zagrożeniami dla zdrowia i działania przeciw chorobom. Dane tam zawarte są niespójne i w części niezaktualizowane[103]. Wszystkie istotne strony są dostępne tylko w wersji angielskiej, co z punktu widzenia zapewnienia realizacji praw podmiotom danych budzi uzasadnione wątpliwości. Kwestie językowe pojawiłyby się również, gdyby doszło do nieuprawnionego przetworzenia danych przez podmiot w państwie innym niż np. obywatelstwa podmiotu danych.

Trudno też jednoznacznie określić, jaki wpływ na efektywność ochrony danych w tym kontekście ma zróżnicowanie prawa krajowego w zakresie surowszych od prawa UE warunków przekazywania danych dotyczących zdrowia; jak również fakt, że prawo krajowe reguluje relacje między personelem medycznym gromadzącym dane np. od pacjentów a właściwymi organami ds. zdrowia publicznego odpowiadającymi za podejmowanie decyzji na poziomie krajowym o wdrażaniu procedury ustalania kontaktów zakaźnych, uczestniczącymi w systemie EWRS i przekazującymi te dane do innych zainteresowanych państw członkowskich.

6. WNIOSKI KOŃCOWE

Obecny system prawa UE przeciwdziałania poważnym, transgranicznym zagrożeniom dla zdrowia realizuje cel ochrony zdrowia przy zapewnieniu ochrony danych osobowych, w tym danych medycznych. Można uznać, że z punktu widzenia spójności regulacji dotyczących równolegle bezpieczeństwa zdrowia i ochrony danych osobowych jest to system przyzwoity, który zapewnia dobry poziom ochrony danych osobowych jednostek. Do tej pory nie jest znany przypadek, kiedy działanie EWRS i procedury ustalania kontaktów zakaźnych między państwami członkowskimi doprowadziłyby do naruszeń prawa do ochrony tych danych. Dotychczasowa praktyka EWRS wskazuje, że z punktu widzenia szybkości i efektywności reagowania oraz ochrony zdrowia publicznego jest to narzędzie, które realizuje założony cel. Jednak, biorąc pod uwagę zapewnianie ochrony danych osobowych, stosowanie decyzji 1082/2013 i działanie EWRS pokazuje też skalę i zakres możliwych transferów danych[104]. Przy naprawdę masowym wdrażaniu środków ustalania kontaktów zakaźnych obowiązujące przepisy mogłyby doprowadzić do naruszeń prawa do ochrony danych z powodu istniejących

[102] Na dzień 31.10.2016. Zalecenie Komisji nr 2012/73, pkt 8.

[103] Badania własne, zob. http://ec.europa.eu/health/preparedness_response/policy/decision/index_ en.htm oraz http://ec.europa.eu/health/communicable_diseases/early_warning/comm_legislation_en.htm (dostęp: 30.09.2016).

[104] Sprawozdanie 2015, s. 9–10.

niedociągnięć (zob. punkt 5.3.). Tym bardziej, że wadą obecnej legislacji unijnej w tym zakresie jest także duża ilość skomplikowanych naukowo i technicznie postanowień rozproszona w wielu podstawowych i wykonawczych aktach prawnych, w których przeciętny obywatel nie jest w stanie zorientować się, jak, przez jakie instytucje i w jakim celu dane są gromadzone czy przetwarzane, dotyczy to zresztą także barier językowych przy kontakcie np. z ECDC. Podstawowym wnioskiem końcowym *de lege ferenda* jest więc przede wszystkim potrzeba wydania brakujących przepisów wykonawczych i delegowanych. Zapewniłoby to zwiększenie kompletności i spójności rozwiązań prawnych w omawianej dziedzinie i tym samym lepiej gwarantowało efektywną ochronę danych osobowych przy stosowaniu przepisów decyzji 1082/2013 o transgranicznych zagrożeniach dla zdrowia.

APPLYING THE RULES ON CROSS-BORDER THREATS TO HEALTH AND THE PROTECTION OF PERSONAL DATA IN THE EU

Summary

The paper concerns a possible conflict between the scope of data protection of individuals, including their medical data, and the necessity of preparing and reacting to serious cross-border health threats at the EU level, for example, to pandemics. The case-study of Mr Andrew Speaker, who was ordered not to leave the US by the US Centre for Disease Prevention and Control because of his TB infection, but was travelling through Europe in 2007, provides an illustration to problematic legal issues. The text presents EU regulatory tools which aim at preventing the spread of infectious diseases and other serious cross-border health threats (as provided by Decision 1082/2013) and the relevant provisions ensuring data protection of individuals in this context. The objective of the extensive normative analysis of the current regulatory framework is an attempt at assessment whether the current system of EU rules can offer an effective protection of personal data when the provisions on pandemics' prevention are applied.

Przegląd Prawa i Administracji 107, 2016