

Europejskie organy ochrony danych osobowych – reforma systemu i nowe wyzwania

Streszczenie

W artykule podjęto problem reformy systemu ochrony danych osobowych w kontekście zmian, nowych zadań i wyzwań stojących przed europejskimi organami ochrony danych, w szczególności Europejskim Inspektorem Ochrony Danych, Grupą roboczą art. 29 czy też krajowymi organami nadzorczymi. Przedłożone w ostatnich latach przez Komisję Europejską projekty aktów ogólnych odnoszących się do omawianych zagadnień, jak i szczególnych, regulujących funkcjonowanie agencji UE zajmujących się walką z przestępczością, wyraźnie pokazują, że zaproponowane zmiany mają służyć zwiększeniu roli tych organów zarówno w wymiarze unijnym, jak i krajowym, poprzez zapewnienie skuteczniejszego egzekwowania nowych przepisów. Temu też służyć ma planowane zacieśnienie współpracy między organami krajowymi i koordynacja ich działań.

Słowa kluczowe: ochrona danych osobowych, organy ochrony danych osobowych, reforma systemu ochrony danych osobowych.

The European personal data protection authorities – the reform of the system and new challenges

Abstract

The article discusses the problem of the reform of the system of the protection of personal data in the context of changes, new tasks and challenges faced by the European data protection authorities, in particular the European Data Protection Supervisor, Article 29 Working Group or the national supervisory authorities. The proposals of regulations and directives submitted in recent years by the European Commission related to data protection in general, as well as the specific rules governing the functioning of the EU agencies involved in the fight against crime clearly show that the proposed changes are

intended to increase the role of these bodies at both the E.U. and the national level by ensuring a more effective implementation of the new rules. The planned strengthening of the relationship between the national authorities as well as the coordination of their activities also aims to meet this objective.

Keywords: personal data protection, data protection authorities, the data protection reform.

W ostatnich latach w Unii Europejskiej podjęto dyskusję, która zmierza do reformy ochrony danych osobowych¹. Poza merytorycznym zakresem prawa do ochrony danych osobowych, zmianom podlegać będą także metody działania organów ochrony danych osobowych, zarówno tych na poziomie Unii Europejskiej (Europejski Inspektor Ochrony Danych czy Grupa art. 29), ale także krajowych organów ochrony danych osobowych².

Ostatnie lata to również wiele wyzwań, przed którymi stanęły organy ochrony danych osobowych, a wśród nich szczególnie widoczne stają się problemy związane z koniecznością wyważenia relacji między prawem do ochrony danych osobowych a obowiązkiem Unii Europejskiej oraz państw członkowskich do zapewnienia obywatelom bezpieczeństwa w ramach przestrzeni wolności i sprawiedliwości. Drugim podstawowym problemem jest konieczność wyważenia prawa do prywatności z wolnością wypowiedzi w kontekście istotnych zmian technologicznych, zwłaszcza upowszechnienia się nowych technologii.

W związku z powyższym, warto przeanalizować zadania i wyzwania, jakie stoją przed organami ochrony danych osobowych w Unii Europejskiej w dwóch kontekstach. Po pierwsze, dyskutowana całościowa reforma systemu ochrony danych osobowych prowadzić może do przyznania nowych funkcji i nowych kompetencji organom unijnym, w szczególności w zakresie działalności agencji UE zajmujących się walką z przestępczością (Europol, Eurojust). Drugi kontekst niniejszego opracowania ma wymiar krajowy – w związku z trwającą procedurą wyboru polskiego Generalnego

¹ Niniejszy artykuł jest wynikiem badań prowadzonych przez autorkę w ramach projektu „Standard ochrony danych osobowych w obszarze współpracy policyjnej i sądowej w sprawach karnych w Unii Europejskiej”, sfinansowanego ze środków Narodowego Centrum Nauki przyznanych na podstawie decyzji numer DEC-2012/07/B/HS5/03908. Szerzej na temat reformy zob. m.in. A. Gajda, *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4, s. 59–92; A. Grzelak, *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstanie jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4, s. 93–126. Zob. także M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014.

² Zob. w szczególności projekty zawarte w dokumentach Komisji COM(2012) 10, COM(2012) 11, COM(2013) 173, COM(2013) 534 oraz COM(2013) 535.

Inspektora Ochrony Danych Osobowych trzeba przywrócić się zadaniom, jakie przed krajowymi organami nadzorczymi stawia prawo UE i zmianom, związanym z reformą systemu w Unii Europejskiej. Trzeba też zwrócić uwagę, że w ostatnim roku pojawiło się wiele ważnych orzeczeń Trybunału Sprawiedliwości Unii Europejskiej (TSUE) dotyczących prawa do prywatności i prawa do ochrony danych osobowych, w tym także odnoszących się do wymogu niezależności organów krajowych (sprawa C-614/10 *Komisja p. Austrii*), co w kontekście projektowanych zmian również wymaga analizy.

Europejski Inspektor Ochrony Danych

Podstawowe zadania

Europejski Inspektor Ochrony Danych (EIOD) został ustanowiony na mocy rozporządzenia nr 45/2001³, które miało uregulować zasady przestrzegania reguł ochrony danych osobowych przez instytucje i organy powołane przez lub na podstawie ówczesnych traktatów ustanawiających Wspólnoty Europejskie (obecnie: Traktat o funkcjonowaniu Unii Europejskiej TFUE). Rozporządzenie nakładało jednocześnie obowiązki związane z ochroną podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do prywatności w odniesieniu do przetwarzania danych osobowych. Zgodnie z art. 1 ust. 2 rozporządzenia 45/2001, niezależny organ nadzoru ustanowiony przez rozporządzenie, zwany Europejskim Inspektorem Ochrony Danych (EIOD, *European Data Protection Supervisor*), monitoruje stosowanie przepisów rozporządzenia do wszystkich operacji przetwarzania danych przeprowadzanych przez instytucje lub organy Wspólnoty (obecnie UE)⁴. Rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez wszystkie instytucje i organy UE, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu UE.

Szczegółowe zadania i uprawnienia EIOD określone zostały w rozdziale V rozporządzenia 45/2001, które jest podstawą funkcjonowania tego niezależnego organu nadzoru. EIOD jest odpowiedzialny przede wszystkim za monitorowanie i zapewnienie zastosowania przepisów rozporządzenia i każdego innego aktu UE,

³ 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. L 8 z 12.1.2001, s. 1–22; dalej jako: rozporządzenie 45/2001.

⁴ Szerzej na temat genezy urzędu EIOD zob. H. Hijmans, *The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority*, "Common Market Law Review" 2006, vol. 43, s. 1313–1342.

odnoszącego się do podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucje i organy UE oraz za doradztwo instytucjom i organom UE oraz podmiotom danych we wszystkich kwestiach związanych z przetwarzaniem danych osobowych.

EIOD powoływany jest na 5-letnią kadencję przez Parlament Europejski i Radę w drodze wspólnego porozumienia, na podstawie listy ustalonej przez Komisję po ogłoszeniu publicznego naboru dla kandydatów⁵, z możliwością ponownego powołania na kolejną kadencję. Wśród cech, jakie musi posiadać EIOD, rozporządzenie wymienia niekwestionowaną niezależność oraz doświadczenie i umiejętności wymagane do spełniania obowiązków. Rozporządzenie reguluje również ogólne warunki wypełniania obowiązków przez EIOD, kwestie związane z personelem i środkami finansowymi⁶.

Szczególnie istotne są jednak te postanowienia, które dotyczą niezależności EIOD. W art. 44 rozporządzenia 45/2001 potwierdza się, że EIOD wykonuje swoje obowiązki w sposób całkowicie niezależny, nie oczekuje i nie przyjmuje instrukcji od nikogo oraz powstrzymuje się od wszelkich czynności niezgodnych ze swoimi obowiązkami, a także podczas swojej kadencji nie wykonuje żadnej innej zarobkowej lub niezarobkowej działalności zawodowej. Również po zakończeniu kadencji EIOD ma obowiązek zachowywać się uczciwie i dyskretnie, jeżeli chodzi o przyjmowanie zleceń czy korzyści. Podlega również obowiązkowi zachowania tajemnicy zawodowej, co jest zrozumiałe ze względu na tematykę, jaką się zajmuje.

Do podstawowych obowiązków EIOD należy z jednej strony rozpatrywanie skarg – z obowiązkiem wysłuchania, zbadania i poinformowania podmiotu danych o wyniku tego postępowania „w odpowiednim czasie” oraz przeprowadzanie dochodzeń, zarówno z własnej inicjatywy, jak i na podstawie skarg, a następnie informowanie podmiotu danych o ich wyniku w rozsądnym czasie. Z drugiej strony EIOD ma zadania związane z procesem opiniowania i stosowania aktów prawnych UE dotyczących ochrony danych osobowych, poprzez monitorowanie i zapewnianie stosowania przepisów rozporządzenia 45/2001 oraz każdego innego aktu UE odnoszącego się do ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucję lub organ UE, z wyjątkiem TSUE, a także doradzanie wszystkim instytucjom i organom UE, albo z własnej inicjatywy, albo w odpowiedzi na konsultacje, we wszystkich kwestiach dotyczących przetwarzania danych osobowych, w szczególności zanim przyjmą one przepisy wewnętrzne związane z ochroną podstawowych praw

⁵ Zgodnie z tą samą procedurą powoływany jest Zastępca EIOD, którym od grudnia 2014 r. jest Polak – były Generalny Inspektor Ochrony Danych w Polsce – dr Wojciech Wiewiórowski.

⁶ Zob. art. 43 rozporządzenia 45/2001.

i wolności w odniesieniu do przetwarzania danych osobowych. Wreszcie, EIOD ma obowiązek monitorować rozwój w odpowiednich dziedzinach, w tym w zakresie technologii informatycznych i telekomunikacyjnych, o ile ma to wpływ na ochronę danych osobowych.

EIOD zobowiązany został do współpracy z krajowymi organami nadzoru, w stopniu koniecznym dla wykonywania ich obowiązków, w szczególności poprzez wymianę wszystkich użytecznych informacji, a także współpracy z organami nadzoru w dziedzinie ochrony danych ustanowionymi w obszarze współpracy policyjnej i sądowej w sprawach karnych UE (w tym wspólnymi organami nadzorczymi działającymi w ramach Europolu i Eurojustu). EIOD uczestniczy też w działalności Grupy roboczej art. 29. Również akty prawne UE inne niż rozporządzenie 45/2001 powierzają EIOD wykonywanie szczegółowych zadań wynikających z dyrektywy 95/46⁷ – w szczególności związanych z wydawaniem zabezpieczeń i upoważnień czy prowadzeniem rejestru operacji przetwarzania.

Dla efektywnej realizacji obowiązków rozporządzenie 45/2001 przyznało EIOD określone uprawnienia, związane z doradzaniem podmiotom danych w kwestii korzystania z ich praw, przekazaniem sprawy administratorowi w wypadku domniemanego naruszenia przepisów rządzących przetwarzaniem danych osobowych i w miarę potrzeb zaproponowaniem środków prawnych dla usunięcia tego naruszenia oraz dla poprawy ochrony podmiotów danych. EIOD może również ostrzec lub upomnieć administratora danych czy też nakazać poprawę, zablokowanie, wykasowanie lub zniszczenie wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów rządzących przetwarzaniem danych osobowych oraz powiadomienie o takich działaniach osób trzecich, którym dane zostały ujawnione, a wreszcie nałożyć czasowy lub całkowity zakaz przetwarzania. EIOD ma także uprawnienia związane z przekazaniem sprawy odpowiedniej instytucji lub organowi UE i, jeśli to konieczne, Parlamentowi Europejskiemu, Radzie i Komisji, a także TSUE zgodnie z postanowieniami traktatów, jak również interweniowaniem w sprawach wniesionych przed TSUE. Dalej rozporządzenie stwierdza, że EIOD ma uprawnienia związane z uzyskaniem od administratora lub instytucji bądź organu UE dostępu do wszystkich danych osobowych i do wszystkich informacji koniecznych dla prowadzonych przez niego dochodzeń oraz do uzyskania dostępu do pomieszczeń, w których administrator lub instytucja bądź organ UE prowadzi działalność, jeżeli są wystarczające powody, aby przypuszczać, że prowadzona jest tam działalność podlegająca rozporządzeniu 45/2001⁸.

⁷ Dyrektywa 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. L 281, 23.11.1995, s. 31; dalej jako: dyrektywa 95/46.

⁸ Zob. art. 47 rozporządzenia 45/2001.

EIOD posiada również kompetencje wynikające z innych aktów prawnych, w szczególności w obszarze przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej. Zastosowany w Systemie Informacyjnym Schengen II (SIS II), a wcześniej w Eurodac⁹ oraz Wizowym Systemie Informacyjnym VIS¹⁰ model kontroli i nadzoru składa się z trzech elementów: po pierwsze, krajowy niezależny organ nadzorczy jest odpowiedzialny za nadzorowanie, czy dane przetwarzane w ramach SIS II na jego terytorium są przetwarzane i przekazywane zgodnie z prawem; po drugie – nadzór nad działaniami krajowego organu nadzorczego sprawuje EIOD. Wreszcie, krajowe organy nadzorcze oraz EIOD współpracują ze sobą i konsultują się dwa razy do roku, podczas spotkań organizowanych przez EIOD. Mają one służyć koordynacji nadzoru nad SIS II, wymianie istotnych informacji, analizowaniu trudności czy badaniu problemów związanych z wykładnią przepisów. Art. 62 decyzji w sprawie SIS II¹¹ ustanawia kilkuwarstwową strukturę nadzoru i odpowiedzialności, rozdzielając zadania między EIOD i krajowe organy nadzorcze. Jest to zmiana w porównaniu do stanu obowiązującego wcześniej. Z kolei w rozporządzeniu w sprawie SIS II¹² jest odwołanie do dyrektywy 95/46 w zakresie uprawnień krajowych organów nadzoru.

Obecnie jednak – co zostało już wspomniane, ale z racji zaproponowanych zmian wymaga ponownego podkreślenia – EIOD nie posiada kompetencji w odniesieniu ani do Eurojustu ani Europolu, które nie podlegają w chwili obecnej przepisom rozporządzenia 45/2001 z racji tego, że były to agencje UE ustanowione na podstawie przepisów ówczesnego Traktatu o Unii Europejskiej, a nie Traktatu ustanawiającego Wspólnotę Europejską.

⁹ Obecnie system Eurodac regulowany jest przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej, złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, a także zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, Dz. Urz. L 180 z 29.06.2013, s. 1.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz. Urz. L 218 z 13.08.2008, s. 60.

¹¹ Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), z uwzględnieniem decyzji 2013/157/UE (data stosowania), Dz. Urz. L 205 z 7.8.2007, s. 63 oraz Dz. Urz. UE L 87 z 27.3.2013, s. 8–9.

¹² Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. L 381 z 28.12.2006, s. 4.

Zmiany przewidziane reformą systemu ochrony danych osobowych w UE

Sam projekt rozporządzenia ogólnego, który ma być podstawowym aktem regulującym zasady ochrony danych osobowych w UE¹³, nie przewiduje żadnych zmian w zakresie działania Europejskiego Inspektora Ochrony Danych z racji tego, że ten akt ma uchylić dyrektywę 95/46, a nie rozporządzenie 45/2001. Projektodawca (Komisja Europejska) zakłada, że przyjmowane rozporządzenie, dyrektywa, obowiązujące rozporządzenie 45/2001 oraz obowiązujące akty szczególne dotyczące wymiany danych w ramach takich organów jak Europol czy Eurojust, będą się wzajemnie uzupełniać¹⁴. Podstawowym problemem, który powinien jednak zostać rozwiązany, a projekty na razie tej kwestii nie podnoszą, jest zatem relacja między obowiązującymi aktami prawnymi. Projekt rozporządzenia ogólnego nie przewiduje ani uchylecia, ani nawet ustanowienia ich hierarchii. Wręcz przeciwnie – pozostawiają one bez uszczerbku wcześniej przyjęte akty prawne¹⁵, a zatem zamiast ujednolicenia – w systemie prawnym UE obowiązywać będzie nadal wiele aktów prawnych regulujących kwestie ochrony danych osobowych¹⁶. Trzeba jednak mieć na uwadze, że rozporządzenie ogólne dość znacząco zmienia system ochrony danych osobowych w UE, co wiązać się będzie z nowymi zadaniami i wyzwaniami stojącymi przez EIOD.

Jednak znaczące zmiany zostały zaproponowane w innych projektach aktów prawnych. Zmiany te polegają przede wszystkim na zwiększeniu zadań EIOD i przyznaniu mu nowych obszarów działalności. Dotyczy to w szczególności objęcia nadzorem działalności Eurojustu i Europolu, a zatem agencji UE utworzonych na mocy Traktatu o Unii Europejskiej w brzmieniu sprzed Traktatu z Lizbony i nieobjętych z tego względu dotychczas postanowieniami rozporządzenia 45/2001. W związku ze zmianami systemowymi, jakie zaszły w UE w kontekście „uwspólnotowienia” obszaru dawnego III filaru UE i nowym brzmieniem przepisów TFUE dotyczących współpracy policyjnej i sądowej w sprawach karnych, Komisja w 2013 r. zaproponowała również

¹³ COM(2012) 11 – Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych); dalej jako: projekt rozporządzenia ogólnego.

¹⁴ Naturalnie, nie obejmą również przetwarzania danych w ramach wspólnej polityki zagranicznej i bezpieczeństwa, objętej inną podstawą traktatową UE.

¹⁵ Por. art. 59 projektu dyrektywy COM(2012) 10 oraz art. 88 i 89 projektu rozporządzenia COM(2012) 11.

¹⁶ W kontekście jednolitości i spójności takiego rozwiązania zob. uwagi A. Grzelak, op.cit., s. 106 i n.

projekty rozporządzeń – nowych aktów prawnych, które regulowałyby działalność Europolu¹⁷ i Eurojustu¹⁸.

Podstawowe zmiany dotyczące systemu ochrony danych osobowych, jakie zaproponowano w wypadku obu agencji, odnoszą się do kwestii zastosowania rozporządzenia 45/2001 do ich działań. Zasadniczo, w rozdziale IV projektu rozporządzenia w sprawie Eurojustu, który dotyczyć będzie przetwarzania informacji, ma znaleźć się odniesienie do rozporządzenia 45/2001. Rozporządzenie 45/2001 ma być podstawowym systemem i standardem przetwarzania wszystkich danych osobowych w Eurojuście, ale projekt rozporządzenia przepisy te uzupełnia tak, by uwzględnić specyfikę działań w zakresie współpracy w sprawach karnych¹⁹. Chociaż rozporządzenie 45/2001 nie jest w żadnym wypadku dostosowane do specyfiki tego obszaru²⁰, to – w opinii EIOD, który odniósł się do przedstawionego projektu – takie rozwiązanie, polegające na uzupełnieniu przepisów rozporządzenia 45/2001 przez szczegółowe przepisy rozporządzenia o Eurojuście, jest słuszne i zasadne²¹.

Eurojust jest agencją UE i z tego względu logiczne jest zastosowanie rozporządzenia 45/2001 do czysto administracyjnego przetwarzania danych, w odniesieniu m.in. do danych osobowych, np. pracowników Eurojustu. Nie ma jednak argumentów uzasadniających zastosowanie go do działań operacyjnych Eurojustu. Przy okazji warto wskazać, że zupełnie inaczej reguluje tę kwestię projekt rozporządzenia dotyczący Europolu, gdzie wyraźnie rozporządzenie 45/2001 będzie miało zastosowanie wyłącznie do kwestii administracyjnych, związanych z zarządzaniem Europolem²². Nie jest jasne, dlaczego pojawiło się takie zróżnicowanie, zwłaszcza że obie agencje współpracują ze sobą w dziedzinie egzekwowania prawa. Komisja również nie wyjaśnia tego w uzasadnieniu. Warto dodać, że także wspólny organ nadzorczy Eurojustu wypowiedział się wielokrotnie przeciwko rozwiązaniu polegającemu na takim podejściu, że rozporządzenie 45/2001 ma być podstawą przetwarzania danych osobowych we wszystkich agencjach UE. Uznał też, że jest to sprzeczne z deklaracją 21 dołączoną do TFUE, bowiem ta przewiduje specyfikę przetwarzania

¹⁷ COM(2013) 173 – Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Współpracy i Szkolenia w Dziedzinie Egzekwowania Prawa (Europol) i uchylające decyzje 2009/371/WSiSW i 2005/681/WSiSW – dalej jako: projekt rozporządzenia w sprawie Europolu.

¹⁸ COM(2013) 535 – Wniosek w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w sprawach karnych (Eurojust) – dalej jako: projekt rozporządzenia w sprawie Eurojustu.

¹⁹ Art. 27 ust. 5 projektu rozporządzenia w sprawie Eurojustu.

²⁰ Pkt 15 preambuły do projektu rozporządzenia w sprawie Eurojustu.

²¹ *Opinion of the European Data Protection Supervisor on the package of legislative measures reforming Eurojust and setting up the European Public Prosecutor's Office ('EPPO')* z 14 marca 2014 r., streszczenie opublikowane w Dz. Urz. UE z 2014 r. C 244, s. 15.

²² Por. punkt 32 i 43 preambuły do projektu rozporządzenia o Europolu.

danych w dziedzinach objętych współpracą w sprawach karnych²³. Z kolei EIOD jest zadowolony z takiego podejścia²⁴.

Istotna zmiana zaproponowana w projekcie rozporządzenia polega na rezygnacji ze wspólnego organu nadzorczego Joint Supervisory Body (JSB) i określeniu obowiązków Europejskiego Inspektora Ochrony Danych (EIOD) w odniesieniu do monitorowania operacji przetwarzania danych osobowych w Eurojuście²⁵. Na podstawie obowiązujących przepisów EIOD nie posiada obecnie żadnych kompetencji w odniesieniu do ochrony danych osobowych w ramach Eurojustu. Podczas prac nad decyzją ramową w sprawie ochrony danych osobowych w ramach karnych, przyjętą później jako decyzja ramowa 2008/977/WSiSW²⁶, próbowano wprowadzić jeden wspólny organ nadzorczy dla Europolu, Eurojustu czy SIS, ale okazało się to niemożliwe z przyczyn politycznych²⁷. Zmienia to zdecydowanie projekt rozporządzenia w sprawie Eurojustu, który odchodzi od wspólnego organu nadzorczego na rzecz EIOD. Zastosowanie będą mieć zatem przepisy ogólne wynikające z rozporządzenia 45/2001, dotyczące ustanowienia czy powoływania EIOD, a także jego niezależności czy ogólnych warunków wypełniania przez niego obowiązków oraz postanowienia dotyczące tajemnicy zawodowej, uprawnień czy obowiązków. Do tego dochodzą jednak postanowienia projektu rozporządzenia, które miałyby przyznać EIOD nowe uprawnienia i kompetencje.

Projekt rozporządzenia w sprawie Eurojustu przewiduje, że EIOD działa w ścisłej współpracy z krajowymi organami właściwymi w zakresie nadzoru ochrony danych w konkretnych kwestiach wymagających krajowego zaangażowania, zwłaszcza w sytuacji, gdy EIOD lub krajowy organ właściwy w zakresie nadzoru ochrony danych stwierdzi znaczące rozbieżności między praktykami państw członkowskich lub potencjalnie niezgodne z prawem przekazanie przy wykorzystaniu kanałów

²³ Opinia Joint Supervisory Body z 14 listopada 2013 r., s. 5. Tekst opinii JSB dostępny jest na stronie http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/jsb/opinions/Opinion%20on%20the%20new%20Eurojust%20Regulation,%202013/OpinionJSB_new_Eurojust_Regulation_2013-11-14_EN.pdf, pobrano 14.12.2014.

²⁴ Zob. streszczenie opinii Europejskiego Inspektora Ochrony Danych w sprawie pakietu środków legislacyjnych reformujących Eurojust oraz ustanawiających Prokuraturę Europejską („EPPO”), (2014/C 244/08), Dz. Urz. C 244 z 2014 r., s. 15.

²⁵ Na tę zmianę zwracają uwagę w szczególności P. de Hert, V. Papakonstantinou, *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, Study requested by the LIBE Committee, European Parliament PE 510.001, Bruksela 2014, s. 15.

²⁶ 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. Urz. L 350 z 30.12.2008, s. 60.

²⁷ Zob. E. de Busser, *Data Protection in EU and US Criminal Cooperation. A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*, Maklu, Antwerpen-Apeldoorn-Portland 2009, s. 183.

komunikacji Eurojustu lub w kontekście kwestii podniesionych przez przynajmniej jeden krajowy organ nadzorczy w sprawie wykonania i interpretacji rozporządzenia o Eurojuście. W tym celu EIOD i organ krajowy może wymieniać się odpowiednimi informacjami, pomagać sobie w przeprowadzaniu kontroli oraz inspekcji, badać trudności w interpretacji czy stosowaniu rozporządzenia, analizować problemy związane z przeprowadzaniem niezależnego nadzoru lub korzystaniem z praw przez osoby, których dane dotyczą, sporządzać zharmonizowane wnioski dotyczące wspólnych rozwiązań wszelkich problemów, a także promować wiedzę na temat praw do ochrony danych, zależnie od potrzeb.

Do EIOD będzie można również składać skargę, której podstawą jest art. 32 ust. 2 rozporządzenia 45/2001, zgodnie z którym każdy podmiot danych może wnieść skargę do EIOD, jeśli uważa, że jego prawa wynikające z traktatu zostały naruszone w wyniku przetwarzania jego danych przez Eurojust. W projekcie rozporządzenia dodaje się, że jeżeli skarga wniesiona na podstawie art. 32 ust. 2 rozporządzenia 45/2001 przez osobę, której dane dotyczą, ma związek z decyzją, o której mowa w art. 32 lub 33, EIOD ma obowiązek zasięgnąć opinii krajowych organów nadzorczych lub właściwego organu sądowego w państwie członkowskim, które było źródłem danych, lub bezpośrednio zainteresowanego państwa członkowskiego. Decyzja EIOD, która może obejmować nawet odmowę przekazania jakichkolwiek informacji, jest podejmowana w ścisłej współpracy z krajowym organem nadzorczym lub właściwym organem sądowym.

Jeżeli skarga dotyczy przetwarzania danych dostarczonych Eurojustowi przez państwo członkowskie, EIOD ma zapewnić prawidłowe przeprowadzenie niezbędnych kontroli w ścisłej współpracy z krajowym organem nadzorczym państwa członkowskiego, które dostarczyło dane. Jeżeli skarga dotyczy przetwarzania danych dostarczonych Eurojustowi przez organy UE, państwa trzecie, organizacje międzynarodowe lub strony prywatne, EIOD dopilnowuje, aby Eurojust przeprowadził niezbędne kontrole.

Wprowadzenie EIOD do systemu nadzoru nad przetwarzaniem danych w Eurojuście budzi wiele wątpliwości, zwłaszcza wspólnego organu nadzorczego Eurojustu (JSB), który wypowiedział się kilkakrotnie na ten temat²⁸. JSB stoi na stanowisku, że Eurojust ma szczególny system ochrony danych, a efektywność nadzoru uzależniona jest od dobrej współpracy inspektora ochrony danych i JSB. JSB uważa także, że Traktat z Lizbony wcale nie wymaga, by wszystkie agencje i instytucje podlegały nadzorowi jednego organu. Nadzór nad działaniami Eurojustu wymaga szczególnej wiedzy sądowej, co gwarantuje obecny skład JSB (sędziowie, wyposażeni w odpowiednie gwarancje niezależności). Konieczna jest również dobra współpraca między krajowymi

²⁸ Por. w szczególności wspomniana wyżej opinia JSB, s. 20–22.

organami ochrony danych – nie gwarantuje tego, zdaniem JSB, proponowany system współpracy EIOD z krajowymi organami ochrony danych. JSB uważa, że skoro EIOD na podstawie art. 46c rozporządzenia 45/2001 nie ma uprawnień do nadzorowania TSUE, to z tych samych względów powinien być wyłączony z nadzorowania Eurojustu. EIOD nie ma również uprawnień do wydawania instrukcji na poziomie krajowym.

W wypadku Europolu, w projekcie rozporządzenia zakłada się – podobnie jak w wypadku Eurojustu – wzmocnienie istniejącego autonomicznego systemu ochrony danych osobowych, a zatem niepodleganie Europolu pod system, który tworzony jest w projekcie dyrektywy o ochronie danych osobowych w sprawach karnych COM(2012) 10²⁹. Jednak inaczej niż w Eurojuście – przetwarzanie osobowych danych administracyjnych, czyli takich, które nie służą realizacji zadań Europolu, a także danych osobowych pracowników Europolu³⁰ ma podlegać zasadom określonym w rozporządzeniu 45/2001. Jest to propozycja odmienna niż w wypadku Eurojustu, gdzie całość działań Eurojustu ma zostać objęta zakresem rozporządzenia 45/2001³¹. Ponownie należy podkreślić, że nie jest jasne, z czego ma wynikać takie rozróżnienie i co je uzasadnia.

Projekt rozporządzenia o Europolu zakłada zwiększenie roli zewnętrznego inspektora ochrony danych w Europolu. EIOD ma mieć właściwość organu nadzoru przetwarzania danych osobowych przez Europol, co – według Komisji Europejskiej – ma zapewnić pełną zgodność z kryteriami niezależności ustalonymi w orzecznictwie TS oraz, ze względu na uprawnienia EIOD do egzekwowania przepisów, skuteczność nadzoru ochrony danych.

Europejski Inspektor Ochrony Danych ma być odpowiedzialny za monitorowanie i zapewnianie stosowania przepisów rozporządzenia odnoszących się do ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych przez Europol. Zadaniem EIOD ma być również doradzanie Europolowi i osobom, których dane dotyczą, we wszelkich sprawach związanych z przetwarzaniem danych osobowych. Projekt rozporządzenia o Europolu szczegółowo określa

²⁹ COM(2012) 10 – Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady 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; dalej jako: projekt dyrektywy o ochronie danych osobowych w sprawach karnych.

³⁰ Por. art. 48 projektu rozporządzenia o Europolu.

³¹ Europejski Inspektor Ochrony Danych „ubolewa”, że w wypadku Europolu zakres obowiązywania rozporządzenia 45/2001 został ograniczony. Por. streszczenie opinii EIOD w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Agencji Unii Europejskiej ds. Współpracy i Szkolenia w Dziedzinie Egzekwowania Prawa (Europol) i uchylającego decyzje 2009/371/WSiSW i 2005/681/WSiSW, Dz. Urz. C 38 z 8.02.2014, pkt 170. Zob. również całą opinię dostępną na stronie EIOD.

jego zadania w art. 46, wskazując m.in. na konieczność prowadzenia dochodzeń z własnej inicjatywy lub na podstawie skarg, a także na monitorowanie i zapewnianie stosowania przez Europol przepisów rozporządzenia. Wskazuje się również, że poza uprawnieniami doradczymi, EIOD będzie mógł ostrzegać lub upominać Europol, nakazywać podjęcie określonych środków, ale także nakładać czasowy lub całkowity zakaz przetwarzania danych osobowych. Będzie również uprawniony do przekazania sprawy TSUE³² czy też Parlamentowi Europejskiemu i Radzie. EIOD będzie również uprawniony do uzyskiwania dostępu do wszelkich danych osobowych i informacji niezbędnych w związku z prowadzonymi przez niego postępowaniami wyjaśniającymi.

EIOD będzie działał w ścisłej współpracy z krajowymi organami nadzorczymi w konkretnych kwestiach, które wymagają zaangażowania krajowego, wymieniając się odpowiednimi informacjami czy też pomagając sobie wzajemnie w przeprowadzeniu kontroli i inspekcji³³. Krajowe organy ochrony danych mają jednak pozostać właściwe do nadzoru wprowadzania, odzyskiwania i wszelkiego przekazywania Europolowi danych osobowych przez zainteresowane państwo członkowskie. Pozostają również odpowiedzialne za sprawdzanie, czy takie wprowadzanie, odzyskiwanie lub przekazywanie narusza prawa osoby, której dane dotyczą. W projekcie rozporządzenia przewiduje się również wprowadzenie elementów „wspólnego nadzoru” nad danymi przekazywanymi Europolowi i przetwarzanymi przez Europol. W konkretnych kwestiach wymagających zaangażowania poszczególnych państw oraz w celu zapewnienia spójnego stosowania niniejszego rozporządzenia w całej UE, EIOD i krajowe organy nadzorcze, działając w ramach swoich kompetencji, powinny również ze sobą współpracować.

Podobnie jak w wypadku Eurojustu, EIOD będzie miał również za zadanie rozpatrywanie skarg. Zakłada się bowiem, że każda osoba, której dane dotyczą, będzie miała prawo do złożenia skargi do EIOD, jeśli uważa, że przetwarzanie dotyczących jej danych nie jest zgodne z przepisami rozporządzenia. Wreszcie, projekt przewiduje, że odwołania od decyzji EIOD będą wnoszone do TS.

Podsumowując, widoczne jest, że nowe zadania postawione przed EIOD będą wiązały się z nowymi kompetencjami w dziedzinie, którą EIOD dotychczas się zajmował wyłącznie w kontekście opiniowania projektów aktów prawnych, czyli w obszarze walki z przestępczością. To może oznaczać konieczność zwiększenia liczby pracowników urzędu i wzmocnienia specjalizacji również w tej istotnej dziedzinie, o ile projekty rozporządzenia o Eurojuście i o Europolu zostaną przyjęte w zaproponowanym

³² Podstawą prawną będzie zapewne art. 263 TFUE.

³³ Por. art. 47 projektu rozporządzenia o Europolu.

kształcie. Sam charakter organu, jakim jest Europejski Inspektor Ochrony Danych nie zmienia się: nie nabiera on właściwości instytucji UE (nie jest wymieniony jako taki w art. 223 i n. TFUE), nie jest agencją UE ani organem regulacyjnym. Nie staje się również wraz z zaproponowanymi zmianami organem sądowym³⁴. Wydaje się, że zmiany w charakterze działania EIOD powinny wiązać się z ewentualną reformą rozporządzenia 45/2001, która jednak obecnie nie jest przeprowadzana. Działalność EIOD ma jednak ogromne znaczenie z tego względu, że gwarantuje niezależność i jakość, która zapewnia, że problematyka ochrony danych osobowych znajduje swój coraz szerszy wyraz w pracach UE i odzwierciedlenie nawet w przepisach traktatowych (art. 16 TFUE), a także wywiera coraz istotniejszy wpływ na kształt przyszłych aktów prawnych UE, chociaż nie zawsze jeszcze opinie EIOD są uwzględniane³⁵.

Grupa robocza art. 29

Podstawowe zadania

Oprócz Europejskiego Inspektora Ochrony Danych organem, który zajmuje się tą problematyką na poziomie Unii Europejskiej jest również tzw. Grupa robocza art. 29. Dyrektywa 95/46 powołała grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Ponieważ jej funkcjonowanie i zadania określa art. 29 dyrektywy, grupa ta nazywana jest właśnie Grupą roboczą art. 29 (Article 29 Working Party). Grupa ta ma charakter doradczy i działa w sposób niezależny, a w jej skład wchodzi przedstawiciele organu lub organów nadzorczych, powołanych przez każde państwo członkowskie oraz przedstawiciel organu lub organów ustanowionych dla instytucji i organów UE, a także przedstawiciel Komisji Europejskiej (Komisji). Zastrzeżono również, że jeżeli państwo członkowskie powoła więcej niż jeden organ nadzorczy, organy te wyznaczają wspólnego przedstawiciela.

Grupa robocza art. 29 podejmuje decyzje zwykłą większością głosów przedstawicieli organów nadzorczych, a do jej zadań należy m.in. badanie każdej kwestii dotyczącej stosowania krajowych środków przyjętych na mocy dyrektywy 95/46, aby przyczynić się w ten sposób do jednolitego stosowania tych środków. Grupa robocza art. 29 przekazuje również Komisji opinie na temat stopnia ochrony danych osobowych w Unii Europejskiej i w państwach trzecich, doradza w sprawie wszelkich

³⁴ Szerzej na temat przyczyn takiego stanowiska zob. H. Hijmans, op.cit., s. 1325 i n.

³⁵ Szerzej na ten temat autorka pisze w *Ochrona danych osobowych ofiar przestępstw w prawie Unii Europejskiej*, w: *Unia Europejska w roli gwaranta i promotora praw podstawowych*, red. D. Kornobis-Romanowska, Wrocław 2014 (w opracowaniu redakcyjnym).

proponowanych zmian dyrektywy, dodatkowych lub szczególnych środków mających na celu zabezpieczenie praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych oraz innych proponowanych środków UE dotyczących praw i wolności, czy też wydawanie opinii na temat kodeksów postępowania opracowywanych na poziomie UE.

Grupa robocza może również z własnej inicjatywy formułować zalecenia we wszystkich sprawach dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych w UE, co w ostatnich latach jest podstawowym działaniem Grupy³⁶. Opinie i zalecenia grupy roboczej są przekazywane Komisji oraz komitetowi wspierającemu Komisję, działającemu na podstawie art. 31 dyrektywy 95/46. Komisja ma obowiązek poinformować grupę roboczą o podejmowanych działaniach w odpowiedzi na opinie i zalecenia komitetu, przedstawiając sprawozdanie przekazywane również Parlamentowi Europejskiemu i Radzie oraz udostępniane opinii publicznej.

Trzeba podkreślić, że w ostatnich latach Grupa robocza art. 29 wydała wiele bardzo istotnych dokumentów, które mają znaczenie w szczególności z praktycznego punktu widzenia i stanowią wskazówkę dla podmiotów stosujących prawo ochrony danych osobowych.

Zmiany przewidziane reformą systemu ochrony danych osobowych

Zmiany w zakresie funkcjonowania Grupy roboczej art. 29 zakładają zarówno projekt rozporządzenia ogólnego COM(2012) 11, jak i projekt dyrektywy dotyczącej ochrony danych osobowych w obszarze spraw karnych COM(2012) 10. Obydwa projekty zawierają przepisy regulujące funkcjonowanie nowego organu, jakim ma być Europejska Rada Ochrony Danych i zakładają zastąpienie Grupy roboczej art. 29 przez Europejską Radę Ochrony Danych (EROD), w skład której mają wejść szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych. Komisja nie będzie członkiem Europejskiej Rady Ochrony Danych, ale będzie miała prawo uczestniczyć w jej działaniach i być w niej reprezentowana.

Europejska Rada Ochrony Danych musi być organem niezależnym, czyli w szczególności nie może podczas wykonywania swoich zadań zwracać się do nikogo o instrukcje ani przyjmować żadnych instrukcji. Obsługę sekretariatu EROD ma zapewniać EIOD, chociaż wydaje się, że sekretariat ten powinien być niezależny. Konieczne jest doprecyzowanie i analiza, jak osiągnąć tę niezależność pod względem praktycznym,

³⁶ Opinie Grupy roboczej art. 29 dostępne są na stronie http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

choćby w wymiarze podległości służbowej. W kontekście samej struktury EROD warto zwrócić uwagę, że nie ma przekonujących powodów, by przyjąć, że to właśnie EIOD powinien pełnić funkcję stałego wiceprzewodniczącego EROD, tak jak proponuje to projekt rozporządzenia.

W art. 66 projektu rozporządzenia ogólnego opisano jej zadania, na podstawie obecnego art. 30 dyrektywy 95/46, ale jednocześnie przedstawiono elementy dodatkowe, odzwierciedlając w ten sposób szerszy zakres działalności Europejskiej Rady Ochrony Danych w Unii i poza nią. Podstawowym zadaniem EROD ma być doradzanie Komisji na temat każdej sprawy związanej z ochroną danych osobowych w Unii, a także badanie z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji każdej kwestii, której zakres obejmuje stosowanie rozporządzenia. EROD będzie też mogła wydawać wytyczne, zalecenia oraz formułować najlepsze praktyki kierowane do organów nadzorczych w celu zachęcenia do spójnego stosowania rozporządzenia. EROD ma także promować współpracę i skuteczną dwustronną oraz wielostronną wymianę informacji, a także praktyk między organami nadzorczymi. Nowością jest wprowadzenie sformułowania, że Komisja będzie mogła wnioskować o wydanie opinii w określonym terminie.

Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania przepisów rozporządzenia na terytorium całej Unii, w tym poprzez doradzanie Komisji i promowanie współpracy organów nadzorczych. Należy stwierdzić, że zasadniczo jej zadania pokrywają się z obecnymi zadaniami Grupy roboczej art. 29. Wzmacnia się jedynie jej struktura poprzez sformalizowanie kwestii związanych z działalnością sekretariatu. Trzeba też pamiętać, że w związku z nowym systemem ochrony danych osobowych rola EROD będzie znacząca, jako że ten organ powinien działać na rzecz jednolitego stosowania prawa UE.

Nowe zadania krajowych organów nadzorczych

Obowiązująca dyrektywa 95/46 w art. 28 zobowiązała państwa członkowskie UE do ustanowienia organów władzy publicznej odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych przez państwa na mocy dyrektywy. Organy te – zgodnie z postanowieniami dyrektywy – muszą funkcjonować w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji.

Dyrektywa zobowiązała również państwa do przyznania tym organom: 1) uprawnień dochodzeniowych, w tym np. prawa dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych, 2) skutecznych uprawnień interwencyjnych, jak np. prawa do wyrażania opinii przed przystąpieniem do operacji

przetwarzania danych zgodnie z art. 20, oraz zapewnienia odpowiedniej publikacji swoich opinii, zarządzania blokady, usunięcia lub zniszczenia danych, nakładania czasowego lub ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub też prawo kierowania sprawy do parlamentów narodowych lub innych instytucji politycznych, 3) prawa pozywania w wypadku naruszenia krajowych przepisów przyjętych zgodnie z dyrektywą. Krajowy organ nadzorczy jest również upoważniony do rozpatrywania skarg zgłaszanych przez dowolną osobę lub przez stowarzyszenie ją reprezentujące, odnośnie do ochrony jej praw i wolności w zakresie przetwarzania danych osobowych.

Projekt rozporządzenia ogólnego nie wprowadza bardzo istotnych zmian. W rozdziale VI odnosi się wyraźnie do kwestii niezależnych organów nadzorczych, zobowiązując państwa w art. 46 do ustanowienia organów nadzorczych. Jednocześnie jednak rozszerza zakres powierzonych im zadań o obowiązek wzajemnej współpracy oraz współdziałania z Komisją Europejską. Art. 47 projektu rozporządzenia wyjaśnia warunki niezależności organów nadzorczych, co stanowi realizację orzeczeń TSUE (sprawa C-518/07³⁷ oraz C-614/10³⁸) i zostało zainspirowane art. 44 rozporządzenia 45/2001³⁹. Zdaniem TSUE, zagwarantowanie niezależności krajowych organów kontroli ma na celu zapewnienie skuteczności i pewności kontroli przestrzegania przepisów w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i powinno być interpretowane w świetle tego celu. Trybunał podkreśla, że „niezależność została przyjęta nie celem przyznania tym organom i ich pracownikom szczególnego statusu, lecz celem wzmocnienia ochrony osób i instytucji, których dotyczą decyzje tych organów. Z tego wynika, że przy wykonywaniu swoich obowiązków organy kontroli powinny działać w sposób obiektywny i bezstronny. W tym celu powinny pozostawać poza jakimkolwiek wpływem z zewnątrz, w tym bezpośrednim czy pośrednim wpływem państwa czy krajów związkowych, a nie tylko poza wpływem organów kontrolowanych”⁴⁰. W konsekwencji organy kontroli właściwe w zakresie przetwarzania danych osobowych w sektorze niepublicznym powinny cechować się niezależnością pozwalającą im na wykonywanie ich zadań bez wpływu z zewnątrz. Ta niezależność wyklucza nie tylko jakikolwiek wpływ ze strony

³⁷ Wyrok Trybunału w sprawie C-518/07 z dnia 9 marca 2010 r. *Komisja Europejska przeciwko Republice Federalnej Niemiec*, ECLI:EU:C:2010:125. Szerzej na temat wyroku zob. H.P. Bull, *Die "völlig unabhängige" Aufsichtsbehörde*, „Europäische Zeitschrift für Wirtschaftsrecht” 2010, s. 488–494.

³⁸ Wyrok Trybunału w sprawie C-614/10 z dnia 16 października 2012 r. *Komisja Europejska przeciwko Republice Austrii*, ECLI:EU:C:2012:631. Szerzej zob. M. Szydło, *Principles underlying independence of national data protection authorities: Commission v. Austria*, „Common Market Law Review” 2013, s. 1809–1826.

³⁹ Projekt rozporządzenia COM(2012) 11, s. 13.

⁴⁰ Zob. ww. wyrok w sprawie C-518/07, pkt 30.

instytucji kontrolowanych, lecz również jakiegokolwiek nakazy i jakiegokolwiek inny wpływ z zewnątrz, bez względu na to, czy bezpośredni, czy pośredni, który mógłby podważyć wykonywanie przez te organy ich zadań, polegających na ustaleniu słusznej równowagi pomiędzy ochroną prawa do poszanowania życia prywatnego a swobodą przepływu danych osobowych.

Trybunał wskazuje także wyraźnie, że samo tylko zagrożenie możliwością wpływu politycznego organów nadzoru na decyzje organów kontroli właściwych w zakresie przetwarzania danych osobowych jest wystarczającą przeszkodą w niezależnym wykonywaniu przez nie zadań. Jako uzasadnienie takiego stanowiska TS podkreśla po pierwsze, możliwość uzyskania „przewidywanego posłuszeństwa” tych organów kontroli w świetle praktyki decyzyjnej organu nadzoru, a po drugie, że rola strażników prawa do poszanowania życia prywatnego, jaką wypełniają te organy kontroli, wymaga, by ich decyzje, a tym samym one same, pozostawały poza jakimkolwiek podejrzeniem stronniczości. Kontrola państwowa wykonywana nad krajowymi organami kontroli właściwymi w zakresie przetwarzania danych osobowych w sektorze niepublicznym jest zatem niezgodna z wymogiem niezależności. W efekcie, państwo członkowskie, poddając nadzorowi państwowemu organy kontroli właściwe w zakresie przetwarzania danych osobowych przez instytucje niepubliczne i przedsiębiorstwa publiczne, działające na konkurencyjnym rynku w niektórych krajach związkowych, i dokonując w ten sposób błędnej implementacji wymogu, zgodnie z którym organy te wykonują zadania „całkowicie niezależnie”, uchybia zobowiązaniom ciążącym na nim na podstawie przepisów obowiązującej dyrektywy.

Organ nadzorczy ma zatem działać w sposób w pełni niezależny podczas wykonywania obowiązków i powierzonych mu uprawnień. Członkowie organu nadzorczego podczas wykonywania swoich obowiązków nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują. Członkowie organu nadzorczego mają obowiązek powstrzymać się od wszelkich czynności niezgodnych ze swoimi obowiązkami podczas swojej kadencji – nie wolno im podejmować żadnej funkcji zarobkowej lub niezarobkowej, stojącej w sprzeczności z tymi obowiązkami. Ostrożność w obejmowaniu stanowisk i przyjmowaniu korzyści zalecana jest również po zakończeniu kadencji. Państwa członkowskie zobowiązane są do zapewnienia, by organ nadzorczy był wyposażony w odpowiednie zasoby ludzkie, techniczne i finansowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania swoich obowiązków i uprawnień, w tym do ich wykonywania w kontekście wzajemnej pomocy, współpracy i uczestnictwa w EROD. Sformułowania te zawarte w projekcie rozporządzenia ogólnego nie są zupełnie przejrzyste i zapewne to TS będzie musiał ocenić, co one oznaczają w wymiarze praktycznym.

Projekt rozporządzenia dodaje także, że każde państwo członkowskie ma obowiązek zapewnić, by organ nadzorczy miał własny personel, który jest powoływany przez szefa tego organu i podlega jego kierownictwu. Wszelka kontrola finansowa, której podlega organ, nie może naruszać jego niezależności. Dodaje także wyraźnie, że członkowie organu nadzorczego mają być wybierani przez parlament albo przez parlament i rząd danego państwa członkowskiego spośród osób, których niezależność jest niekwestionowana oraz których doświadczenie i umiejętności w dziedzinie ochrony danych osobowych zostały wykazane. Nie krytykując próby zagwarantowania w ten sposób niezależności od organów rządowych, można jedynie podać ją w wątpliwość i stwierdzić, że właściwie nie jest jasne, dlaczego nie dopuszczono udziału innych podmiotów, jak chociażby rady sądownictwa. Przepisy rozporządzenia określają również przesłanki odwołania lub pozbawienia określonych praw członka organu nadzorczego.

W osobnej sekcji rozdziału VI projektu rozporządzenia określono kompetencje organów nadzorczych. Zasadę ogólną, określoną obecnie w art. 28 ust. 6 dyrektywy 95/46 (kompetencje na terytorium własnego państwa członkowskiego), uzupełnia nowa kompetencja organu głównego w wypadku, gdy administrator lub podmiot przetwarzający ma siedzibę w kilku państwach członkowskich, co ma zapewnić jednolitość stosowania („punkt kompleksowej obsługi” – tzw. *one-stop shop*). Sądy, w zakresie sprawowanych funkcji sądowniczych, będą zwolnione z kontroli organu nadzorczego, lecz nie będą zwolnione ze stosowania materialnych przepisów dotyczących ochrony danych.

Art. 52 projektu rozporządzenia ogólnego określa obowiązki organu nadzorczego, w tym dotyczące rozpatrywania skarg i prowadzenia postępowań w ich sprawie oraz szerzenia w społeczeństwie wiedzy na temat ryzyka, przepisów, gwarancji i praw. Nie wskazano wyraźnie, chociaż wydawałoby się to konieczne, że organy powinny mieć również wyraźnie określone kompetencje do prowadzenia audytów w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych⁴¹. Z kolei w art. 53 projektu rozporządzenia ogólnego określa się uprawnienia organu nadzorczego, wzorując się zasadniczo na obecnym art. 28 ust. 3 dyrektywy 95/46 i art. 47 rozporządzenia 45/2001, ale jednocześnie dodaje się kilka nowych elementów, w tym uprawnienie do nakładania sankcji administracyjnych. Trzeba podkreślić, że sankcje określone w art. 79 i n. projektu rozporządzenia ogólnego są wysokie i mają doprowadzić do harmonizacji zasad stosowania sankcji administracyjnych w tym obszarze.

Kolejny rozdział projektu rozporządzenia ogólnego dotyczy współpracy organów nadzorczych i mechanizmu zgodności – art. 55 wprowadza jasne przepisy

⁴¹ Zob. opinię Grupy roboczej art. 29, s. 18.

dotyczące obowiązkowej wzajemnej pomocy, przedstawiając skutki braku zastosowania się do żądania innego organu nadzorczego. Przewidziano również możliwość dokonywania wspólnych operacji, co – jak wynika z uzasadnienia do projektu – zostało zainspirowane przez przepisy decyzji Rady 2008/615/WSiSW⁴². W takich wspólnych operacjach mogą wziąć udział również organy nadzorcze. W szczególności, na podstawie art. 56 rozporządzenia, po jego przyjęciu w celu zacieśnienia współpracy i zwiększenia wzajemnej pomocy organy nadzorcze wykonują wspólne zadania dochodzeniowe, przyjmują wspólne środki egzekucyjne i prowadzą inne wspólne operacje, podczas których wyznaczeni członkowie lub personel organów nadzorczych z innych państw członkowskich uczestniczą w operacjach na terytorium danego państwa członkowskiego⁴³.

Krajowy organ nadzorczy będzie również uczestniczył w tzw. mechanizmie zgodności, dotyczącym podejmowanych przez organy nadzorcze środków, których oddziaływanie co do zasady rozciąga się na obszar wykraczający poza granice danego państwa członkowskiego. Projekt środka nadzorczego miałby być przesłany przez organ nadzorczy do zaopiniowania Komisji i EROD, którym (w szczególności Komisji) przysługiwałyby w tym zakresie również pewne uprawnienia decyzyjne. Jest to nowy mechanizm, którego celem jest ponownie zapewnienie jednolitego stosowania prawa na terytorium całej UE.

W kontekście problematyki tworzenia polityki publicznej, omawiane organy mają za zadanie zwrócić uwagę na czynniki wpływające na tworzenie się polityki publicznej w różnych dziedzinach, z uwzględnieniem elementów prywatności i potrzeby ochrony danych osobowych. Zarówno EIOD, jak i Grupa robocza art. 29 (przyszła EROD) czy też krajowe organy nadzorcze, muszą zwracać szczególną uwagę na zmienność polityki publicznej, jej priorytetów i metod osiągnięcia celów w kontekście stojących przed nimi zadań.

Ujmując politykę publiczną jako dziedzinę systemowych, uporządkowanych działań państwa podejmowanych w celu rozwiązywania kluczowych problemów zbiorowych, należy wskazać, że omawiane w tym artykule organy przyczyniają się do kształtowania różnych ich aspektów, ale zawsze z uwzględnieniem polityki prywatności. Ponieważ głównymi narzędziami tworzenia polityki są regulacje prawne, ale także samoregulacje, ocena i interpretacja przyjmowanych w UE aktów prawnych

⁴² Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. L 210 z 6.08.2008, s. 12.

⁴³ Szczegółowe zasady określono w art. 59 projektu rozporządzenia ogólnego.

wpływają na zakres ich zastosowania oraz tworzą pozytywne bodźce do przyjmowania oczekiwanych postaw.

Podsumowując powyższe rozważania, można dodać, że zmiany dotyczące organów nadzorczych są istotnym elementem reformy europejskich ram prawnych ochrony danych osobowych. Zwiększenie ich roli ma zapewnić skuteczniejsze egzekwowanie przepisów. Temu też służyć ma planowane zacieśnienie współpracy między organami krajowymi i koordynacja ich działań. Zmieniona zostanie również płaszczyzna współpracy przy uwzględnieniu, że obecna aktywność Grupy roboczej art. 29 nie zawsze pozwala na skuteczne egzekwowanie przepisów.

Przed polskim GODO stoją zatem wyzwania związane ze stosowaniem i implementacją nowych przepisów unijnych, w wymiarze nowych zadań, ale także konieczności ścisłej współpracy z innymi organami krajowymi, EIOD czy EROD. Również władze publiczne stoją przed koniecznością spełnienia wymogu niezależności krajowego organu nadzorczego, poprzez zapewnienie mu warunków gwarantujących prawidłowe funkcjonowanie⁴⁴. Wymóg zapewnienia właściwych warunków, w tym w aspekcie finansowym, jest jednym z elementów niezależności i prawidłowego funkcjonowania organów krajowych.

Bibliografia

- Bull H.P., *Die „völlig unabhängige“ Aufsichtsbehörde*, „Europäische Zeitschrift für Wirtschaftsrecht“ 2010.
- Busser de E., *Data Protection in EU and US Criminal Cooperation. A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*, Maklu, Antwerpen–Apeldoorn–Portland 2009.
- Gajda A., *Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4.
- Grzelak A., *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstanie jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4.
- Hert de P., Papakonstantinou V., *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, Study requested by the LIBE Committee, European Parliament PE 510.001, Bruksela 2014.
- Hijmans H., *The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority*, „Common Market Law Review” 2006, vol. 43.

⁴⁴ Por. problemy wskazane w sprawozdaniach rocznych z działalności GODO, dotyczące w szczególności budżetu urzędu, infrastruktury oraz zasobów ludzkich. Sprawozdania dostępne są na stronie http://www.godo.gov.pl/138/id_art/2685/j/pl/, pobrano 15.02.2015.

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych w obecnym i nadchodzącym stanie prawnym*, Warszawa 2014.

Ochrona danych osobowych ofiar przestępstw w prawie Unii Europejskiej, w: *Unia Europejska w roli gwaranta i promotora praw podstawowych*, red. D. Kornobis-Romanowska, Wrocław 2014.

Szydło M., *Principles underlying independence of national data protection authorities: Commission v. Austria*, "Common Market Law Review" 2013.