PANOPTYKON
FUNDACJA

Zarząd: Katarzyna Szymielewicz, Małgorzata Szumańska
Rada programowa: Adam Bodnar, Ewa Charkiewicz, Dominika Dörre-Nowak, Józef Halbersztadt, Joanna Kamiol, Monika Płatek, Maciej Ślusarek, Piotr Waglowski, Roman Wieruszewski

Warszawa, 12 marca 2012 r.

Uwagi Fundacji PANOPTUKON do projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

W odpowiedzi na zaproszenie Ministerstwa Administracji i Cyfryzacji do zgłaszania uwag do projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej**: projekt rozporządzenia**) przedstawiamy swoje wstępne stanowisko. Zastrzegamy jednocześnie, że – ze względu na relatywnie krótki czas konsultacji – nasza analiza nie jest kompletna. Mamy nadzieję, że okazja do zgłoszenia pogłębionych uwag pojawi się jeszcze na dalszych etapach konsultacji.

PYTANIE 1

Czy Państwa zdaniem dotychczasowa dyrektywa należycie odpowiada nowym warunkom, czy też widzą Państwo potrzebę ustanowienia bardziej całościowej i spójnej polityki w zakresie podstawowego prawa do ochrony danych osobowych?

Nie. Coraz szybszy przepływ informacji zawierających dane osobowe, dalej idące możliwości łączenia i wymiany informacji, upowszechnienie korzystania z Internetu i rozwój nowych narzędzi internetowych – wszystkie te zmiany technologiczne oraz społeczne stwarzają nowe wyzwania dla ochrony prywatności i danych osobowych, na które dotychczasowa dyrektywa i – stanowiąca jej implementację do polskiego porządku prawnego – ustawa o ochronie danych osobowych nie dają odpowiedzi.

Czy widzą Państwo wartość dodaną w dalszej harmonizacji obowiązujących w poszczególnych państwach członkowskich UE przepisów o ochronie danych?

Zdecydowanie tak. Ma ona znaczenie nie tylko z punktu widzenia zwiększenia pewności prawnej przedsiębiorców, ale również z punktu widzenia realizacji standardów ochrony praw i wolności obywateli Unii Europejskiej.

PYTANIE 2

Czy proponowane w projekcie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych rozwiązania spełniają oczekiwania w zakresie ochrony danych i tworzenia rynku wewnętrznego?

Kompleksowa reforma prawa ochrony danych osobowych jest w obecnej sytuacji bardzo po-

trzebna. Ogólny kierunek zmian zaproponowany w projekcie rozporządzenia oceniamy pozytywnie. W szczególności wyrażamy poparcie dla następujących propozycji:

- zaostrzenia wymogów dotyczących zgody na przetwarzanie danych osobowych (przede wszystkim wymóg uzyskania zgody wyraźnej, a nie domniemanej);
- zmiany zasad stosowania prawa Unii Europejskiej w stosunku do podmiotów zagranicznych (objęcie podmiotów oferujących swoje usługi obywatelom UE lub monitorujących ich zachowanie, np. w Internecie);
- próbie uregulowania kwestii mających szczególne znaczenie w przypadku usług internetowych (np. takich jak profilowanie czy możliwość przenoszenia danych między serwisami);
- próbie zwiększenia roli organów ochrony danych, w szczególności nadanie wyraźnego uprawnienie do stosowania sankcji administracyjnych w postaci grzywny przez organy nadzorcze.

Mimo dobrego kierunku zmian projekt rozporządzenia wymaga jednak dopracowania w wielu kwestiach szczegółowych, aby zrealizowanie jego ambitnych założeń było możliwe. Szczególną uwagę należy zwrócić na luki prawne, szerokie wyłączenia (uchylające co do zasady dobre rozwiązania prawne[1]) i niektóre problemy strukturalne. Większość z nich staramy się opisać niżej.

Utrzymanie odrębnych reżimów ochrony danych osobowych

Propozycja reformy prywatności zaproponowana przez Komisarz Reding nie rozwiązuje problemu współistnienia odrębnych reżimów ochrony danych osobowych. Obok projektu rozporządzenia mamy projekt dyrektywy o ochronie danych przez organy egzekwowania prawa oraz odrębny reżim przewidziany dla samych instytucji unijnych, który ma być utrzymany (istniejące rozporządzenie o ochronie danych przez instytucje unijne). Dodatkowo, zarówno projekt rozporządzenia jak i dyrektywy przewiduje bardzo szerokie wyłączenie podyktowane względami bezpieczeństwa narodowego (*vide* punkt niżej).

Nawet w razie powodzenia przygotowywanej reformy ogólny kształt europejskiego reżimu ochrony danych pozostanie bardzo skomplikowany i nie unikniemy poważnych rozbieżności w standardach pomiędzy 27 państwami członkowskimi. Szczególnie w odniesieniu do zasad przewidzianych w projekcie dyrektywy, o wiele lepszym rozwiązaniem byłoby przejście na poziom reguł bezpośrednio obowiązujących, czyli rozporządzenia. Nie ma też przeciwskazań, aby zasady przewidziane w projekcie rozporządzenia dla podmiotów prywatnych odnosiły się bezpośrednio do instytucji unijnych, kiedy występują one w charakterze administratorów danych (pracodawców, grantodawców itp.).

Zakres zastosowania i relacje z innymi przepisami prawa

Nasze wątpliwości budzi zakres zastosowania zasad wyrażonych w projekcie rozporządzenia. Jak zaznaczyliśmy wyżej, jest on poważnie ograniczony przez fakt utrzymania odrębnego reżimu prawnego dla organów egzekwowania prawa i instytucji unijnych oraz szerokie wyłączenia podyktowane względami bezpieczeństwa narodowego.

Zgodnie z art. 2 „niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego". Natomiast w preambule (pkt 16) czytamy: „Ochrona osób

[1] Np. do prawa wniesienia sprzeciwu (art. 19 ust. 1).

fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania albo w celu wykonywania kar kryminalnych oraz swobodnym przepływem takich danych podlegają szczególnemu instrumentowi prawnemu na szczeblu Unii. Z tego względu niniejsze rozporządzenie nie powinno mieć zastosowania do przetwarzania do wyżej wspomnianych celów".

Dodatkowo, w samym projekcie rozporządzania znajdują się liczne postanowienia budzące wątpliwości co do jego zakresu zastosowania, zarówno w aspekcie materialnym, jak i terytorialnym. Omawiamy je krótko niżej.

Zgodnie z art. 2 ust. 3 „niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności zasad odpowiedzialności usługodawców będących pośrednikami, o których mowa w art. 12-15 tej dyrektywy". To zastrzeżenie budzi poważne wątpliwości. Nie jest dla nas jasne, w jaki sposób ograniczenia odpowiedzialności pośredników wynikające ze wspomnianej dyrektywy mogą wpłynąć na poszanowanie standardów ochrony prywatności wynikających z projektu rozporządzenia. Pojawia się np. wątpliwość, czy zwolnienie wyszukiwarek od odpowiedzialności na podstawie art. 14 dyrektywy nie wpłynie negatywnie na możliwość zrealizowania uprawnień podmiotu danych wynikających z art. 17 projektu rozporządzenia (usuwanie kopii danych osobowych w związku z realizacją tzw. prawa do zapomnienia). W naszej opinii Komisja Europejska powinna doprecyzować tę kwestię w taki sposób, aby postanowienia dyrektywy 2000/31/WE były stosowane pomocniczo w stosunku do postanowień rozporządzenia.

Treść art. 2 została ponadto zmieniona w toku prac nad projektem i nastąpiło poszerzenie wyłączenia ze względu na tzw. cele osobiste lub domowe. Jeśli utrzyma się obecne brzmienie tego przepisu, zasady wyrażone w rozporządzeniu nie znajdą zastosowania w przypadku przetwarzania danych „przez osobę fizyczną w celach innych niż zarobkowe w ramach własnych działań o charakterze czysto osobistym lub domowym". Wcześniejsza wersja projektu przewidywała istotne ograniczenie tego wyłączenia, mianowicie w przypadkach, gdy dane osobowe są udostępniane nieograniczonej liczbie osób. To zawężenie miało na celu uwzględnienie takich sytuacji, jak przetwarzanie danych osobowych za pośrednictwem publicznie dostępnych forów lub portali społecznościowych. W naszej opinii powrót do dość szerokiego wyłączenia, jakie już dziś przewiduje obowiązująca dyrektywa o ochronie danych, jest błędem.

Pojawiają się też wątpliwości co do zakresu terytorialnego rozporządzenia. W art. 3 ust 1 powraca niejasne sformułowanie „w kontekście działalności", które już wcześniej było przedmiotem krytyki ze strony Grupy Roboczej Art. 29 (właśnie ze względu na możliwe rozbieżności w interpretacji): „niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w kontekście działalności prowadzonej w zakładzie administratora lub podmiotu przetwarzającego na terytorium Unii".

W art. 3 ust. 2 zostało natomiast użyte sformułowanie "oferowanie towarów i usług": „niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych podmiotów danych mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii, gdy przetwarzanie wiąże się z oferowaniem towarów lub usług takim podmiotom danych w Unii".

Na tym tle pojawia się wątpliwość, czy projektowane rozporządzenie ma być stosowane jedynie w przypadku oferowania usług komercyjnych, czy także w przypadku działalności niekomercyjnej oraz nieodpłatnego świadczenia usług (przy założeniu, że zysk jest wypracowywany w inny

sposób, np. z przychodów reklamowych). W naszej opinii niekomercyjny lub nieodpłatny charakter usług nie powinien mieć wpływu na zakres zastosowania ogólnych zasad ochrony danych osobowych, jednak projekt w obecnym kształcie tej kwestii nie rozstrzyga.

Kolejny problem, który wymaga doprecyzowania, to relacja pomiędzy projektem rozporządzenia a Konwencją nr 108 o ochronie danych (która jest jedynym wiążącym międzynarodowym instrumentem prawnym otwartym dla państw z Europy i spoza niej). Wyklarowanie relacji między tymi instrumentami może być szczególnie istotne w kontekście zasad transferu danych do tzw. krajów trzecich. Projekt rozporządzenia przewiduje bowiem rozwiązania, które mogą skutkować przyjmowaniem w takich sytuacjach niższych standardów ochrony danych, niż wynikające z Konwencji nr 108.

Tłumaczenie rozporządzenia

Rozporządzenie będzie obowiązywać w polskim porządku prawnym bezpośrednio, dlatego zasadnicze znaczenie będzie miała jakość jego tekstu. Aby jego stosowanie w praktyce nie budziło niepotrzebnych wątpliwości interpretacyjnych, powinno nie tylko odpowiadać w sposób maksymalnie spójny brzmieniu rozporządzenia w innych językach, ale również realizować zasady techniki prawodawczej w zakresie wykorzystania języka prawnego oraz zasady poprawnej polszczyzny. Niestety projekt rozporządzenia nie spełnia w sposób zadowalający żadnego z tych warunków. Zaproponowane tłumaczenie może budzić wątpliwości nie tylko na poziomie interpretacji pojęć (np. definicja zgody), ale również pod kątem *stricte* językowym (np. tytuł art. 6 – "Zgodność z prawem przetwarzania").

Czy istnieją aspekty ochrony danych i tworzenia rynku wewnętrznego, które w niedostatecznym stopniu lub w ogóle nie zostały poruszone w ramach projektu Rozporządzenia?

Tak. W tym miejscu omówimy dwa przykłady, choć z pewnością można znaleźć ich więcej.

W projekcie rozporządzenia nie pojawiła się propozycja jasnego uregulowania zasad wykorzystywania danych zbieranych (pierwotnie) w celach komercyjnych na potrzeby bezpieczeństwa publicznego (np. w ramach systemów PNR czy reżimu obowiązkowej retencji danych telekomunikacyjnych). Autorzy projektu podjęli próbę uregulowania tej materii w pierwszym projekcie dyrektywy o ochronie danych przez organy egzekwowania prawa (art. 4), jednak te przepisy zostały wykreślone z wersji aktualnie poddawanej konsultacjom. Natomiast zasady zaproponowane w projekcie rozporządzenia są albo zbyt ogólne albo bardzo ograniczone w oddziaływaniu za pomocą szerokich wyłączeń. Tym samym propozycja Komisarz Reding nie próbuje zmierzyć się z problemem pozyskiwania danych komercyjnych do celów związanych z bezpieczeństwem publicznym i egzekwowaniem prawa.

Innym istotnym problemem, który nie znalazł adekwatnego rozwiązania w projekcie, jest transfer danych do krajów trzecich w celach związanych z bezpieczeństwem publicznym i egzekwowaniem prawa. Praktyka w tym zakresie jest bardzo niepokojąca. Szczególne zagrożenia dla ochrony praw podmiotów danych wiążą się z przetwarzaniem danych w chmurze obliczeniowej, gdy dostawcy tego typu usług mają siedziby poza granicami UE. Na przykład, zgodnie z amerykańską ustawą *Foreign Intelligence Surveillance Act* z 2008 roku (art. 1881a), rząd amerykański może prowadzić szeroko zakrojoną inwigilację obywateli innych państw w oparciu o dane przetwarzane przez amerykańskie firmy dla celów politycznych (czyli nawet bez żadnego podejrzenia o działalność przestępczą). Projekt rozporządzenia nie przewiduje żadnych konkretnych

gwarancji w tym kontekście, a jednocześnie stwarza daleko idące ułatwienia w transferze danych osobowych do krajów trzecich (np. w postaci tzw. Wiążących Reguł Korporacyjnych).

PYTANIE 3

Jakie są punkty krytyczne proponowanych rozwiązań?

Definicja zgody

Pozytywnie oceniamy zmiany w podejściu dotyczącym rozumienia zgody na przetwarzanie danych osobowych zmierzające w kierunku wskazania, że zgoda powinna być wyrażona w sposób wyraźny, nie może być milcząca czy dorozumiana oraz, że nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w sytuacji wyraźnego braku równowagi między podmiotem danych a administratorem (pkt 34 preambuły). Warto jednak zwrócić uwagę na elementy definicji (np. słowo "szczególne"), którą są niejasne i mogą w praktyce budzić poważne wątpliwości interpretacyjne.

Zmiana celu przetwarzania

Art. 6 ust. 4 projektu rozporządzenia stanowi, że jeśli cel dalszego przetwarzania nie jest zgodny z celem, dla którego zebrano dane osobowe, przetwarzanie musi opierać się na co najmniej jednej z podstaw prawnych przewidzianych w ust. 1 lit. a)-e) tego artykułu. Jest to rozwiązanie znacznie lepsze od przewidzianego we wcześniejszej wersji projektu rozporządzenia, jednak w naszej opinii nadal nie gwarantuje odpowiedniego standardu ochrony danych. Stanowi ono poszerzenie możliwości dopuszczalnych na gruncie obecnej dyrektywy, dla których nie widzimy dostatecznego uzasadnienia.

Co więcej, art. 14 rozporządzenia nie przewiduje obowiązku poinformowania podmiotu danych o tym, że cel przetwarzania uległ zmianie. Na istnienie takiego obowiązku wskazuje wprawdzie brzmienie preambuły (pkt 40)[2], jednak brak wyraźnego ustanowienia takiego obowiązku w treści projektu rozporządzenia może prowadzić to tego, że w praktyce nie będzie on przez administratorów danych respektowany.

Anonimizacja danych

Rozporządzenie przewiduje, że dane osobowe powinny być „przechowywane w formie umożliwiającej identyfikację podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane są przetwarzane" (art. 5 lic. e). Oznacza to, że zasada ograniczenia czasowego nie odnosi się do przypadków, kiedy dane zostaną poddane anonimizacji. Warto podkreślić, że przy aktualnym rozwoju technologicznym jednoznaczna ocena, czy anonimizacja została dokonana w sposób skuteczny (czyli w sposób nieodwracalny, tak że informacje przetwarzane przez administratora nie pozwalają na zidentyfikowanie osoby), nie jest prosta ani oczywista. Dlatego w naszej ocenie „przechowywane w formie umożliwiającej identyfikację podmiotów danych" nie powinno w sposób automatyczny wyłączać danych spod reżimu ochronnego, szczególnie dopóki

[2] „Jeśli ten inny cel nie jest zgodny z celem pierwotnym, w którym dane zostały zebrane, administrator powinien uzyskać zgodę podmiotu danych na realizację tego celu lub powinien oprzeć przetwarzanie na innej uzasadnionej podstawie zgodnego z prawem przetwarzania, w szczególności przewidzianej przez prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. W każdym przypadku należy zapewnić stosowanie zasad wskazanych w niniejszym rozporządzeniu, w szczególności w zakresie poinformowania podmiotu danych o tych innych celach".

warunki, jakie powinna spełniać skuteczna anonimizacja, nie zostaną jasno sprecyzowane w rozporządzeniu.

Prawo do zapomnienia

Prawo do usunięcia i zaprzestania przetwarzania danych (w przypadku przetwarzania w sposób niezgodny z rozporządzeniem) jest jednym z fundamentalnych praw podmiotu danych. Szczególne problemy związane z respektowaniem tego prawa występują w przypadku treści umieszczonych w Internecie. Dlatego – w celu wzmocnienia tego prawa w przestrzeni Internetu – art. 17 ust. 2 przewiduje, że administrator, który upublicznił dane osobowe ma obowiązek poinformować osoby trzecie przetwarzające te dane, że podmiot danych wnioskuje o usunięcie linków do danych, kopii lub replikacji tych danych osobowych. Przepis ten jednak w praktyce może budzić poważne wątpliwości i wymaga doprecyzowania. W szczególności wyrażenie „wszelkie uzasadnione kroki, w tym środki techniczne" może stwarzać pole do różnorakich interpretacji.

Definicja profilowania i zakres wyłączeń

Na poparcie zasługuje próba uregulowania praktyk profilowania i przyjęcie zasady, że osoba może być poddana profilowaniu tylko w określonych przewidzianych prawem sytuacjach. Niestety brzmienie art. 20 ust. 1, który określa, jakie działania poddane będą temu ograniczeniu, rodzi poważne zastrzeżenia. W szczególności wątpliwości budzi wyrażenie „wywołuje skutki prawne dotyczące tej osoby fizycznej lub ma istotny wpływ na tę osobę fizyczną". W naszej opinii określenie to jest zbyt wąskie i może prowadzić do nieuzasadnionego ograniczenia zastosowania zasad wyrażonych w art. 20.

Niepokoi nas również zakres wyłączeń z zakazu profilowania, przede wszystkim przesłanka, o której mowa w art. 20 ust. 2 lit. a. Zgodnie z tym przepisem profilowanie ma być dopuszczalne „w trakcie zawierania lub wykonania umowy, jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został zrealizowany lub jeśli przewidziano właściwe środki w celu zabezpieczenia słusznych interesów podmiotu danych, jak np. prawo do uzyskania interwencji ze strony człowieka". To bardzo szerokie i trudne do uzasadnienia wyłączenie może zniweczyć sens i cel tego przepisu. Obywatele powinni mieć zapewnioną ochronę przed profilowaniem także w sytuacjach związanych z zawieraniem i realizacją umowy. To bardzo newralgiczny obszar, szczególnie jeśli weźmiemy pod uwagę usługi ubezpieczeniowe lub adresowane do osób małoletnich. Ograniczenie możliwości profilowania w oparciu o dane wrażliwe nie niweluje w pełni generowanych w tych przypadkach zagrożeń.

Współadministratorzy

Art. 24 stanowi, że "jeśli administrator określa cele, warunki i środki przetwarzania danych osobowych wspólnie z innymi administratorami, współadministratorzy danych ustalają zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z niniejszego rozporządzenia spoczywającej na każdym z nich, w szczególności jeśli chodzi o procedury i mechanizmy wykonania praw podmiotu danych, w drodze wspólnych ustaleń". W naszej opinii przyjęcie takiego rozwiązania stwarza ryzyko obniżenia standardu ochrony danych osobowych przewidzianego w rozporządzeniu w drodze umowy między współadministratorami. Wszyscy administratorzy powinni być zobowiązani do zachowania pewnych minimalnych standardów.

Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych

Pozytywnie oceniamy propozycję wprowadzenia obowiązku zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych (art. 32 ust. 1). Rozwiązanie to nie tylko zwiększa jego kontrolę nad przetwarzaniem danych osobowych i umożliwia podjęcie środków zaradczych w przypadku np. ujawnienia danych osobowych, ale może mieć również pozytywny wpływ na bezpieczeństwo przetwarzanych danych (poprzez zwiększenie „samokontroli" administratorów danych, którzy będą mieli świadomość, że informacja o naruszeniu ochrony danych osobowych dotrze do podmiotu danych).

Niestety pozytywny walor proponowanej regulacji może być zniweczony przez brzmienie art. 32 ust. 3, który zakłada, że „zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych nie jest wymagane, jeśli administrator wykaże, zgodnie z wymogami organu nadzorczego, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie ochrony danych osobowych". Takie ograniczenie nie ma uzasadnienia, zwłaszcza w zestawieniu z brzmieniem ust. 1: trudno sobie wyobrazić sytuację, w której zostaje spełniona przesłanka z ust. 3 (administrator wdraża odpowiednie środki ochrony), a jednocześnie aktualne zostaje zagrożenie, o którym mowa w ust. 1.

Szczególne ryzyko dla praw i wolności

Pozytywnie oceniamy próbę uregulowania operacji, które stwarzają szczególne ryzyko dla praw i wolności podmiotów danych. Niestety zaproponowany w projekcie rozporządzenia mechanizm uważamy za niewystarczający z punktu widzenia neutralizacji tych zagrożeń. Art. 33 stanowi, że „jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych". Ocena ta nie jest jednak poddawana żadnej zewnętrznej weryfikacji, co sprawia, że trudno ją uznać (o ile w ogóle powstanie) za rzeczywistą próbę oceny skutków wpływu przewidywanych operacji na ochronę danych. Praktyczny wymiar gwarancyjny tej regulacji może być zatem bardzo ograniczony.

Na uwagę zasługuje również brzmienie ust. 5, który w sposób nie do końca jasny ogranicza stosowanie obowiązku wskazanego w ust. 1[3].

Przedstawiciele administratorów niemających siedziby w Unii Europejskiej

Zgodnie z art. 25 ust. 2, obowiązek ustanowienia przedstawiciela administratora danych, który ma siedzibę poza terytorium Unii Europejskiej, nie ma zastosowania w przypadku przedsiębiorstw zatrudniających mniej niż 250 osób. W naszej opinii kryterium liczby osób zatrudnionych w przedsiębiorstwie jest w tym kontekście dość arbitralne i może stwarzać poważne wątpliwości interpretacyjne. Mogą się pojawić zasadnicze wątpliwości, czy na przykład osoby zatrudnione na podstawie umów zlecenia lub umów o współpracy zaliczają się do osób „zatrudnionych" w świetle tego artykułu. Ponadto nie jest dla nas jasne, jaki związek ma liczba osób zatrudnionych w przedsiębiorstwie z wymaganym przez UE standardem „rozliczalności" (obowiązek ustanowienia przedstawiciela w UE ma służyć realizacji tej zasady). Może się przecież

[3] Ograniczenie wynikające z tego przepisu stanowi natomiast kolejny argument, który powinien przemawiać za przyjęciem zasady, że projekty aktów prawnych powinny zawierać ocenę wpływu projektowanych regulacji na ochronę praw i wolności w sferze prawa do prywatności i ochrony danych osobowych.

okazać, że stosunkowo niewielka firma prowadzi działalność zakładającą przetwarzanie danych na szeroką skalę (np. świadczenie usług związanych z reklamą behawioralną lub innych usług o charakterze *stricte* marketingowym). W tym kontekście sensowniejszym kryterium mogłaby być wysokość rocznych obrotów firmy.

W naszej opinii Komisja Europejska powinna zweryfikować kryterium, od którego uzależnia konieczność wyznaczenia przedstawiciela administratora danych w przypadku przedsiębiorstw niemających siedziby w UE i wyraźnie uzasadnić jego przydatność w tym kontekście.

Transfer danych do krajów trzecich

Poza ogólnymi uwagami przedstawionymi w odpowiedzi na pytanie drugie (transfer danych do krajów trzecich w celach związanych z bezpieczeństwem i egzekwowaniem prawa), mamy parę uwag szczegółowych co do rozwiązań dotyczących transferu danych do krajów trzecich.

Bardzo niepokojący jest zakres wyłączeń od ogólnych reguł, które mają chronić prawa podmiotów danych w przypadku transferu danych poza terytorium UE. W szczególności, zwracamy uwagę na niezwykle szerokie wyłączenie, jakie zostało zaproponowane w art. 44 ust. 1 lit. h). Ten przepis zezwala na transfer danych bez zachowania odpowiednich gwarancji (przewidzianych w art. 41 i 42), jeśli „przekazanie jest konieczne dla potrzeb wynikających ze słusznych interesów administratora lub podmiotu przetwarzającego, których nie można uznać za częste lub masowe i jeżeli administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące operacji przekazywania danych lub operacjom przekazywania danych i na podstawie tej oceny w razie potrzeby przewidzieli odpowiednie gwarancje w zakresie ochrony danych osobowych". W naszej opinii zaproponowana podstawa swobodnego transferu danych poza granice UE jest zbyt szeroka i może otworzyć pole do poważnych nadużyć.

Ponadto w kontekście transferu danych do krajów trzecich niepokojące jest przyznanie Komisji Europejskiej szerokich uprawnień w postaci wydawania aktów delegowanych w celu doprecyzowania pojęć i kryteriów zawartych w art. 44 (*vide* dalsze uwagi na temat art. 86). W ust. 7 czytamy, że „Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania znaczenia „istotnego interesu publicznego" w rozumieniu ust. 1 lit. d), a także kryteriów i wymogów dotyczących odpowiednich gwarancji, o których mowa w ust. 1 lit. h)".

Dotychczasowe doświadczenie z konstrukcjami prawnymi takimi, jak *Safe Harbour* pokazuje, że należy zachować daleko idącą ostrożność w stosowaniu szybkich i uproszczonych mechanizmów transferu danych poza granice UE. Okazuje się, że nie zawsze są one równie przyjazne z punktu widzenia podmiotów ochrony danych osobowych, co z perspektywy samych przedsiębiorców. Z tego samego powodu, obecne uprawnienia Komisji Europejskiej w zakresie kształtowania tych mechanizmów wydają się nam zbyt szerokie.

Właściwość terytorialna organów ochrony danych

Art. 51 uzależnia właściwość terytorialną organów ochrony danych od siedziby nie tyle samego przedsiębiorstwa, co administratora danych lub podmiotu przetwarzającego dane: „w przypadku gdy przetwarzanie danych osobowych odbywa się w kontekście działalności administratora lub podmiotu przetwarzającego ustanowionych na terytorium Unii, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim, organ nadzorczy głównej siedziby administratora lub podmiotu przetwarzającego jest odpowiedzialny za

nadzór nad działalnością administratora lub podmiotu przetwarzającego we wszystkich państwach członkowskich, bez uszczerbku dla przepisów rozdziału VII niniejszego rozporządzenia".

Mimo że takie rozwiązanie wydaje się być uzasadnione (z punktu widzenia organu ochrony danych istotne są działania podejmowane właśnie przez administratora danych, a nie np. właściciela przedsiębiorstwa), mogą się pojawić wątpliwości interpretacyjne – szczególnie w przypadku dużych podmiotów gospodarczych, które prowadzą wiele biur na terenie UE. Projekt nie daje odpowiedzi na pytanie, w jaki sposób konkretne ograny ochrony danych miałyby weryfikować, czy na terytorium podległym ich nadzorowi znajduje się "główna siedziba" nie samego przedsiębiorstwa, ale administratora danych lub podmiotu przetwarzającego dane w ramach konkretnej korporacji. Wydaje się, że – aby ustalić tę okoliczność – krajowe organy ochrony danych musiałyby nie tylko przeprowadzać kontrole lokalnie, ale także współpracować ściśle z organami nadzorczymi z innych państw członkowskich UE.

Kolejny problem, jaki rodzi się na tle art. 51, to uwzględnienie interesów samych podmiotów danych. To rozwiązanie musi doprowadzić do pojawienia się sytuacji, w których podmiot danych w celu wniesienia skargi na działanie konkretnego przedsiębiorcy będzie zmuszony kontaktować się z organem ochrony danych w innym państwie członkowskim. Projekt powinien zatem uwzględnić dodatkowe potrzeby, jakie mogą się pojawić na tym tle po stronie podmiotów danych (np. prawo do wniesienia skargi we własnym języku lub uzyskania od „własnego" organu ochrony danych niezbędnych informacji kontaktowych czy wsparcia procesowego).

Egzekwowanie prawa przez organy ochrony danych w sytuacjach transgranicznych – mechanizmy współdziałania

W porównaniu ze stanem obecnym, mechanizmy współdziałania organów ochrony danych osobowych przewidziane w rozdziale VII (sekcja 1 i 2) stanowią krok w dobrym kierunku. Nie ulega wątpliwości, że potrzebna jest pewna przeciwwaga po stronie organów nadzorczych w stosunku do firm-administratorów danych, które działają w sposób transgraniczny (nierzadko w zasięgu globalnym).

W naszej opinii zaproponowane rozwiązanie jest jednak oparte na dość skomplikowanej i biurokratycznej procedurze, która może nie zdać egzaminu w kontekście wyzwań, jakie generuje transgraniczne egzekwowanie prawa (wysokie koszty postępowań, duża presja czasu i złożoność spraw, rozbieżności językowe itp.). Zgodnie z projektem rozporządzenia, jeden lub dwa organy ochrony danych osobowych będą zmuszone mierzyć się z nierzadko ogromnymi kosztami postępowań, które nie będą w żaden sposób rekompensowane. Podobny problem dotyczy zasobów kadrowych i intelektualnych.

Trudno zakładać, że każdy z krajowych organów ochrony danych – bez względu na wielkość kraju i rozmiar nadzorowanego rynku – będzie dysponował odpowiednimi zasobami, aby poprowadzić skomplikowaną i być może precedensową sprawę przeciwko którejś z globalnych korporacji wyspecjalizowanych w przetwarzaniu danych osobowych. Z drugiej strony, ta spodziewana nierówność w dostępności odpowiednich zasobów może prowadzić do zjawiska zwanego *forum shopping* w odniesieniu do działań nadzorczych (globalne firmy będą chętniej poddawać się nadzorowi „słabszych" organów nadzorczych).

Dlatego w naszej opinii zaproponowane rozwiązanie nie jest optymalne (nie zapewnia odpowiedniej przeciwwagi po stronie organów ochrony danych w stosunku do potężnych, ponadnarodowych korporacji). Rozwiązaniem bardziej efektywnym (oczywiście wyłącznie w odniesieniu do podmiotów działających w skali ponadnarodowej) byłoby powołanie wyspecjalizowanego,

centralnego organu nadzorczego, który działałby w ścisłej współpracy z krajowymi organami ochrony danych osobowych. Można również rozważyć wprowadzenie instytucji „wspólnego dochodzenia" w uzasadnionych, transgranicznych przypadkach naruszenia prawa.

Prawo do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu

Bardzo pozytywnie przyjęliśmy wprowadzenie dodatkowego, sądowego środka ochrony prawnej w przypadku naruszenia praw podmiotów danych. W art. 75 czytamy: „bez uszczerbku dla jakiegokolwiek dostępnego administracyjnego środka ochrony prawnej, w tym prawa do złożenia skargi do organu nadzorczego, o której mowa w art. 73, każda osoba fizyczna ma prawo do sądowego środka ochrony prawnej, jeżeli uznaje, że jej prawa na podstawie niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jej danych osobowych w warunkach niezgodnych z niniejszym rozporządzeniem".

Jest to zdecydowanie krok w dobrym kierunku. Z drugiej jednak strony, projekt nie przewiduje konkretnych gwarancji, które są niezbędne, żeby nadać temu nowemu prawu realny wymiar (np. prawo do skorzystania z ojczystego języka czy prawo do bezpłatnej pomocy prawnej). W różnych krajach te gwarancje, wynikające ze sposobu ukształtowania postępowania cywilnego, mają różny poziom, co musi prowadzić do faktycznego zróżnicowania pozycji osób, które chciałyby z takiego środka ochrony prawnej skorzystać (niekoniecznie we własnym kraju).

Prawo do wniesienia skargi przeciwko zagranicznemu organowi ochrony danych

Artykuł 74, w którym mowa o prawie podmiotu danych do wniesienia skargi sądowej przeciwko organowi ochrony danych, w ust. 4 przewiduje sytuację, w której w imieniu podmiotu danych działa „lokalny" organ nadzorczy: „podmiot danych, którego dotyczy decyzja organu nadzorczego w innym państwie członkowskim niż to, w którym podmiot danych ma miejsce zwykłego pobytu, może zażądać, aby organ nadzorczy państwa członkowskiego, w którym ma miejsce zwykłego pobytu, wszczął postępowanie w jego imieniu przeciwko właściwemu organowi nadzorczemu w innym państwie członkowskim".

W kontekście praktycznych doświadczeń, a także innych postanowień rozporządzenia, które przewidują ścisłą współpracę organów ochrony danych, to rozwiązanie może nie zdać egzaminu. W praktyce trudno sobie wyobrazić występowanie jednego organu ochrony danych przeciwko drugiemu na drodze sądowej, w interesie pojedynczego obywatela. Lepszym pomysłem, w tym kontekście, mogłoby być zaangażowanie, po stronie obywatela, niezależnego rzecznika.

Uprawnienia Komisji Europejskiej do wydawania aktów o charakterze *quasi*-ustawodawczym

Art. 86 projektu rozporządzenia potwierdza uprawnienie Komisji Europejskiej do wydawania aktów o charakterze nieustawodawczym o powszechnym zakresie stosowania, które uzupełniają lub zmieniają niektóre, inne niż zasadnicze, elementy aktu ustawodawczego (akty *quasi*-ustawodawcze). Bezpośrednie odwołania do tej szczególnej kompetencji Komisji pojawiają się w wielu newralgicznych miejscach projektu rozporządzenia (np. w części dotyczącej transferu danych do krajów trzecich, sankcji administracyjnych, prawa do zapomnienia czy przetwarzania danych w celach badawczych bez zgody podmiotu danych).

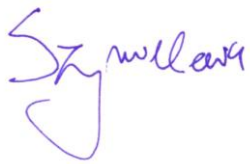
Wydaje się, że te kompetencje Komisji powinny zostać szczegółowo zrewidowane i ograniczone do sytuacji, w których jednostronna decyzja tego organu nie będzie w stanie wpłynąć negatyw-

nie na poziom ochrony danych osobowych zagwarantowany w projekcie rozporządzenia. W wielu przypadkach są to kwestie zbyt ważne i zbyt ściśle związane ze sferą praw i wolności obywatelskich, aby mogły być pozostawione w gestii samej Komisji Europejskiej. Doświadczenie pokazuje, że formalna „procedura sprawdzająca", realizowana przez Parlament Europejski, nie jest w stanie zniwelować tych zagrożeń.

Uprawnienia Komisji Europejskiej w ramach tzw. procedury zgodności

W ramach przewidzianej w rozporządzeniu procedury zgodności, art. 59 daje Komisji Europejskiej prawo do wyrażania opinii „w celu zapewnienia właściwego i spójnego stosowania rozporządzenia". Jak wynika z ust. 2, organ nadzorczy ma obowiązek uwzględnić tę opinię „w jak najszerszym stopniu". Mamy zasadnicze wątpliwości, czy tak daleko idące uprawnienie nie ograniczy suwerenności krajowych organów ochrony danych. Dodatkowo wydaje się, że uprawnienia przyznane Komisji w ramach procedury zgodności stwarzają ryzyko nadmiernego jej wydłużenia.

W imieniu Fundacji PANOPTYKON,



Katarzyna Szymielewicz
Dyrektorka

Małgorzata Szumańska
Członkini Zarządu