Opinia Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie integralności i przejrzystości rynku energii

(2011/C 279/03)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając Kartę praw podstawowych Unii Europejskiej, w szczególności jej art. 7 i 8,

uwzględniając 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 ([1]),

uwzględniając 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 ([2]), w szczególności jego art. 41,

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

I. WPROWADZENIE

1. Dnia 8 grudnia 2010 r. Komisja Europejska przyjęła wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie integralności i przejrzystości rynku energii ([3]) („wniosek").

2. Komisja nie przeprowadziła konsultacji z EIOD, choć wymaga tego art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Działając z własnej inicjatywy, EIOD wydaje niniejszą opinię w oparciu o art. 41 ust. 2 tego rozporządzenia. EIOD zdaje sobie sprawę z faktu, że niniejsza porada udzielona zostaje na późnym etapie procesu legislacyjnego. Uznaje jednak wydanie niniejszej opinii za zasadne i przydatne ze względu na istotny potencjalny wpływ wniosku na prawo do prywatności i ochronę danych osobowych. Na niniejszą opinię należy również powołać się w preambule wniosku.

3. Zasadniczym celem wniosku jest przeciwdziałanie manipulacjom na rynku i wykorzystaniu informacji wewnętrznych na hurtowych rynkach energii (gazu i energii elektrycznej). Integralność i przejrzystość rynków hurtowych, na których odbywa się obrót gazu i energii elektrycznej pomiędzy przedsiębiorstwami produkującymi energię a przedsiębiorstwami handlowymi, mają kluczowe znaczenie dla cen, jakie ostatecznie płacą konsumenci.

4. W tym celu wniosek dąży do ustanowienia kompleksowych zasad na poziomie unijnym w celu uniemożliwienia przedsiębiorstwom handlowym wykorzystywania informacji wewnętrznych dla własnych korzyści oraz manipulowania rynkiem poprzez sztuczne kształtowanie cen powyżej poziomu uzasadnionego dostępnością, kosztem produkcji oraz pojemnością magazynową lub zdolnością przesyłu energii. Proponowane zasady zakazują w szczególności:

   — wykorzystania informacji wewnętrznych w ramach sprzedaży lub zakupu energii na poziomie rynku hurtowego; informacje posiadane na wyłączność i mające wpływ na cenę należy ujawnić przed zawarciem transakcji,

   — transakcji będących źródłem nieprawdziwych lub wprowadzających w błąd sygnałów na temat podaży, popytu lub cen produktów energetycznych sprzedawanych w obrocie hurtowym, oraz

   — rozpowszechniania nieprawdziwych informacji lub plotek na temat takich produktów.

5. Za monitorowanie rynku na poziomie europejskim w celu wykrywania ewentualnych przypadków naruszenia powyższych zakazów odpowiadać będzie Agencja ds. Współpracy Organów Regulacji Energetyki („ACER") ([4]).

6. Zgodnie z wnioskiem, ACER uzyska szybki dostęp do danych na temat transakcji zawieranych na hurtowych rynkach energii. Dotyczy to informacji na temat ceny, wielkości sprzedaży oraz zaangażowanych stron. Taki zasób danych będzie również udostępniany krajowym organom regulacyjnym, które w dalszej kolejności będą zobowiązane do badania podejrzeń o nadużycie. W przypadkach powodujących skutki transgraniczne ACER będzie uprawniona do koordynowania dochodzeń. Krajowe organy regulacyjne w państwach członkowskich będą nakładały kary finansowe.

7. Wniosek jest kolejnym z wielu innych niedawnych wniosków legislacyjnych mających wzmocnić istniejące uzgodnienia w zakresie nadzoru finansowego oraz poprawę koordynacji i współpracy na poziomie unijnym, do których należy dyrektywa w sprawie wykorzystywania poufnych informacji i manipulacji na rynku („MAD") ([5]) i dyrektywa

([1]) Dz.U. L 281 z 23.11.1995, s. 31 (zwana dalej: „dyrektywa 95/46/WE").
([2]) Dz.U. L 8 z 12.1.2001, s. 1 (zwana dalej: „rozporządzenie (WE) nr 45/2001").
([3]) COM(2010) 726 wersja ostateczna.
([4]) ACER jest organem Unii Europejskiej utworzonym w 2010 r. Do jej obowiązków należy pomoc krajowym organom regulacji energii w wykonywaniu na poziomie unijnym zadań regulacyjnych realizowanych w państwach członkowskich oraz, w zależności od potrzeby, koordynacja ich działań.
([5]) Dyrektywa 2003/6/WE Parlamentu Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie wykorzystywania poufnych informacji i manipulacji na rynku (nadużyć na rynku), Dz.U. L 96 z 12.4.2003, s. 16.

w sprawie rynków instrumentów finansowych („MiFID") ([1]). EIOD przedstawił ostatnio uwagi na temat innego ze wspomnianych niedawnych wniosków ([2]).

II. UWAGI I ZALECENIA EIOD

8. Wniosek zawiera wiele przepisów istotnych z punktu widzenia ochrony danych osobowych:

— art. 6–8 dotyczące monitorowania rynku i przekazywania danych,

— art. 9 dotyczący „ochrony danych i niezawodności operacyjnej",

— art. 10 i 11 dotyczące prowadzenia dochodzeń i egzekwowania przestrzegania przepisów, oraz

— art. 14 dotyczący „stosunków z państwami trzecimi".

II.1. **Monitorowanie rynku i przekazywanie danych (art. 6–8)**

Odnośne przepisy

9. Podstawę wniosku stanowi założenie, że w celu wykrywania nadużyć na rynku (i) konieczny jest skutecznie działający system monitorowania rynku z szybkim dostępem do kompletnych danych na temat transakcji, oraz że (ii) powinien on obejmować monitorowanie na poziomie unijnym. W związku z tym, w proponowanym rozporządzeniu przydzielono ACER zadanie gromadzenia, weryfikacji oraz udostępniania (właściwym organom krajowymi i unijnym) znacznej ilości danych ogólnych pochodzących z hurtowych rynków energii.

10. W szczególności, proponowane rozporządzenie zobowiązuje uczestników rynku do przekazywania ACER „danych na temat zawieranych transakcji", których przedmiotem są produkty energetyczne sprzedawane w obrocie hurtowym. Oprócz danych na temat transakcji uczestnicy rynku zobowiązani są również do przekazywania ACER informacji dotyczących „zdolności produkcyjnej instalacji, ich pojemności magazynowej, wielkości zużycia energii lub zdolności przesyłu energii elektrycznej lub gazu ziemnego".

11. Forma i treść przewidzianych informacji oraz termin ich przekazywania określone zostaną w aktach delegowanych Komisji.

Uwagi i zalecenia EIOD

12. Biorąc pod uwagę fakt, że kwestię określenia treści informacji, które mają być gromadzone w ramach realizacji powyższych zadań monitorowania rynku oraz przekazywania danych, rozporządzenie pozostawia w całości aktom delegowanym, nie można wykluczyć, że będą to również dane osobowe – tj. wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej ([3]). Zgodnie z obowiązującym prawem unijnym, jest to dozwolone wyłącznie w sytuacji, gdy jest to konieczne i proporcjonalne do danego celu ([4]). Proponowane rozporządzenie powinno zatem jasno określać, czy i w jakim stopniu dane na temat transakcji i zdolności, które mają być gromadzone dla celów monitorowania, mogą zawierać dane osobowe ([5]).

13. Jeżeli przewidziane jest przetwarzanie danych osobowych, mogą być również wymagane szczególne zabezpieczenia – np. dotyczące celowości, okresu zatrzymania i potencjalnych odbiorców informacji. Ze względu na ich istotny charakter, zabezpieczenia z zakresu ochrony danych należy określić bezpośrednio w tekście proponowanego rozporządzenia, nie zaś w aktach delegowanych.

14. Jeżeli natomiast nie planuje się przetwarzania danych osobowych (bądź takie przetwarzanie miałoby wyłącznie charakter wyjątku i ograniczałoby się do rzadkich przypadków, gdy przedsiębiorca zajmujący się hurtową sprzedażą energii nie jest osobą prawną, lecz fizyczną), powinno zostać to jednoznacznie określone we wniosku – przynajmniej w jednym z motywów.

II.2. **Ochrona danych i niezawodność operacyjna (art. 9)**

Odnośne przepisy

15. Zgodnie z art. 9 ust. 1 ACER „zapewnia poufność, integralność i ochronę" informacji otrzymanych na podstawie art. 7 (tj. danych na temat transakcji i zdolności gromadzonych w ramach realizacji zadania monitorowania rynku). Artykuł 9 przewiduje również, iż „w stosownych przypadkach" podczas przetwarzania danych na podstawie art. 7 ACER „stosuje się" do przepisów rozporządzenia (WE) nr 45/2001.

16. Ponadto ACER, także na podstawie art. 9 ust. 1, „określa źródła ryzyka operacyjnego i ogranicza je poprzez opracowanie odpowiednich systemów, mechanizmów kontroli i procedur".

17. Wreszcie, art. 9 ust. 2 zezwala ACER na podawanie do wiadomości publicznej części informacji będących w jej posiadaniu, „pod warunkiem że nie zostaną ujawnione wrażliwe informacje handlowe dotyczące poszczególnych uczestników rynku lub poszczególnych transakcji".

([1]) Dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych zmieniająca dyrektywę Rady 85/611/EWG i 93/6/EWG i dyrektywę 2000/12/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 93/22/EWG, Dz.U. L 145 z 30.4.2004, s. 1.

([2]) W kwestii szerszego kontekstu powiązanych wniosków legislacyjnych zob. opinia EIOD w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, partnerów centralnych i repozytoriów transakcji, wydana dnia 19 kwietnia 2011 r.; w szczególności jej pkt 4, 5 i 17–20.

([3]) Zob. art. 2 lit. a) dyrektywy 95/46/WE i art. 2 lit. a) rozporządzenia (WE) nr 45/2001.

([4]) Zob. art. 6 ust. 1 lit. c) i art. 7 lit. c) dyrektywy 95/46/WE i art. 4 ust. 1 lit. c) oraz art. 5 lit. b) rozporządzenia (WE) nr 45/2001.

([5]) Artykuł 9 ustęp 1 wniosku – odwołujący się do rozporządzenia (WE) nr 45/2001 – sugeruje, że tak może być w istocie, choć przepis nie zawiera żadnych dalszych szczegółów. W tej kwestii zob. również dział II.2 niniejszej opinii.

Uwagi i zalecenia EIOD

18. EIOD z uznaniem przyjmuje fakt, że art. 9 częściowo poświęcony jest ochronie danych, oraz że proponowane rozporządzenie zawiera szczególny wymóg przestrzegania przez ACER przepisów rozporządzenia (WE) nr 45/2001.

a) Zastosowanie rozporządzenia (WE) nr 45/2001 i dyrektywy 95/46/WE

19. W nawiązaniu do powyższego stwierdzenia EIOD podkreśla, że rozporządzenie (WE) nr 45/2001 ma zastosowanie do ACER w całości, na mocy tegoż rozporządzenia, w każdym przypadku przetwarzania przez nią danych osobowych. Z tego względu we wniosku należy przypomnieć, że rozporządzenie (WE) nr 45/2001 powinno mieć zastosowanie do ACER nie tylko w przypadku przetwarzania przez nią danych na podstawie art. 7, ale również we wszelkich innych sytuacjach – co istotne, również w przypadku przetwarzania przez ACER danych osobowych w związku z podejrzeniem nadużycia na rynku/naruszenia przepisów prawa na podstawie art. 11. Ponadto, dla uściślenia, EIOD zaleca zastąpienie terminu „w stosownych przypadkach" na określenie sytuacji, gdy ACER obowiązana jest stosować się do przepisów rozporządzenia (WE) nr 45/2001, frazą „w każdym przypadku, gdy przetwarzane są dane osobowe".

20. Należy również odnieść się do dyrektywy 95/46/WE, z uwagi na fakt, że dotyczy ona przetwarzania danych osobowych przez zainteresowane krajowe organy regulacyjne. Mianowicie, dla zachowania jasności, EIOD zaleca wskazanie w treści proponowanego rozporządzenia, w sposób ogólny (przynajmniej w jednym z motywów), na fakt, że o ile ACER podlega rozporządzeniu (WE) nr 45/2001, o tyle w przypadku zainteresowanych krajowych organów regulacyjnych zastosowanie ma dyrektywa 95/46/WE.

b) Rozliczalność

21. EIOD z uznaniem przyjmuje wymóg, zgodnie z którym ACER ma określać źródła ryzyka operacyjnego i ograniczać je poprzez opracowanie odpowiednich systemów, mechanizmów kontroli i procedur. Aby dodatkowo wzmocnić zasadę rozliczalności [1], w przypadku, gdyby przetwarzanie danych osobowych miało odgrywać rolę strukturalną, proponowane rozporządzenie powinno zawierać szczególny wymóg stworzenia przez ACER jasnych ram rozliczalności zapewniających zgodność z zasadami ochrony danych i dowody takiej zgodności. Tego rodzaju jasne ramy stworzone przez ACER powinny obejmować wiele elementów, takich jak:

— przyjęcie i aktualizowanie w miarę potrzeby polityki ochrony danych na podstawie oceny skutków (w tym również oceny ryzyka bezpieczeństwa). Taka polityka ochrony danych powinna również zawierać plan bezpieczeństwa,

— przeprowadzanie okresowych kontroli pod kątem stałej adekwatności i zgodności z polityką ochrony danych (w tym kontrole planu bezpieczeństwa),

— podawanie do wiadomości publicznej (przynajmniej częściowo) wyników takich kontroli w celu zapewnienia zainteresowanych stron o zgodności z zasadami ochrony danych, oraz

— informowanie inspektora ochrony danych Komisji, zainteresowanych osób, których dotyczą dane, a w razie konieczności innych zainteresowanych stron i organów, o przypadkach naruszenia zasad ochrony danych i innych incydentach związanych z bezpieczeństwem [2].

22. Analogiczne wymogi powinny mieć zastosowanie w przypadku krajowych organów regulacyjnych i innych zainteresowanych organów unijnych.

c) Upublicznianie informacji przez ACER

23. W związku z wymogiem określonym w art. 9 ust. 2, zgodnie z którym ACER powinna podawać do wiadomości publicznej części informacji będących w jej posiadaniu, EIOD przyjmuje, że celem tego przepisu nie jest zezwolenie ACER na upublicznianie danych w celu „napiętnowania" sprawcy, ani na publiczne ujawnianie bezprawnych działań przedsiębiorstw lub osób fizycznych.

24. Co więcej, we wniosku nie poruszono kwestii ewentualnego zamiaru publicznego ujawniania danych osobowych. Z tego względu, dla uniknięcia wszelkich wątpliwości, proponowane rozporządzenie powinno wyraźnie określać, że upublicznianie informacje nie powinny zawierać danych osobowych, albo precyzować, jakie dane mogą być ewentualnie ujawnianie.

25. W przypadku, gdy mają być upubliczniane dane osobowe, potrzebę ich ujawnienia (np. ze względów przejrzystości) należy dokładnie rozważyć i zestawić z innymi konkurencyjnymi względami, jak potrzeba ochrony przysługującego zainteresowanym osobom prawa do prywatności i ochrony danych osobowych.

26. Stosownie do powyższego, przed każdym przypadkiem ujawnienia danych należy dokonać oceny proporcjonalności, przy uwzględnieniu kryteriów określonych przez Europejski Trybunał Sprawiedliwości w sprawie *Schecke* [3]. W tym przypadku ETS podkreślił, iż odstępstwa i ograniczenia ochrony danych osobowych muszą ograniczać się do tego, co absolutnie konieczne. Ponadto ETS uznał, że instytucje europejskie powinny zbadać inne metody upubliczniania w celu znalezienia takiej, która

[1] Zob. pkt 7 opinii EIOD w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów – „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", wydanej dnia 14 stycznia 2011 r. (tekst w języku angielskim: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

[2] Zob. pkt 6.3 powyższej opinii EIOD z dnia 14 stycznia 2011 r.

[3] Wyrok ETS z dnia 9 listopada 2010 r., sprawy połączone C-92/09 i C-93/09 (*Schecke i Eifert*); zob. zwłaszcza pkt 81, 65 i 86.

będzie zgodna z celem upublicznienia, przy jak najmniejszej ingerencji w prawa osoby, której dotyczą dane, do życia prywatnego i ochrony danych osobowych.

II.3. **Uprawnienia dochodzeniowe (art. 10)**

Odnośne przepisy

27. Wniosek przewiduje, iż monitorowanie rynku będzie połączone z dochodzeniem w przypadku, gdy występuje podejrzenie nadużycia na rynku, oraz że może to prowadzić do zastosowania odpowiednich sankcji. Artykuł 10 ustęp 1 wymaga w szczególności przyznania przez państwa członkowskie koniecznych uprawnień dochodzeniowych krajowym organom regulacyjnym w celu zapewnienia stosowania przepisów rozporządzenia dotyczących wykorzystywania informacji wewnętrznych i manipulacji na rynku ([1]).

Uwagi i zalecenia EIOD

28. EIOD z uznaniem przyjmuje zapis w art. 10 ust. 1, zgodnie z którym (i) uprawnienia dochodzeniowe wykonuje się (wyłącznie) w celu zapewnienia stosowania przepisów rozporządzenia dotyczących wykorzystania informacji poufnych i manipulacji na rynku (art. 3 i 4) oraz (ii) uprawnienia te wykonuje się w proporcjonalny sposób.

29. Co więcej, autorzy wniosku powinni pójść o krok dalej w celu zagwarantowania pewności prawa i stosownego poziomu ochrony danych osobowych. Jak zostanie wykazane poniżej, z proponowanego brzmienia art. 10 wynikają dwa poważne problemy. Po pierwsze, art. 10 nie określa wystarczająco jasno zakresu uprawnień dochodzeniowych; nie jest np. wystarczająco jasne, czy można żądać udostępnienia rejestrów prywatnych rozmów telefonicznych lub czy można przeprowadzać kontrole na miejscu w prywatnym mieszkaniu. Po drugie, art. 10 nie zapewnia koniecznych zabezpieczeń proceduralnych przed ryzykiem nieuzasadnionego naruszenia prywatności lub niewłaściwego wykorzystania danych osobowych; nie przewidziano np. wymogu uzyskania nakazu od organu sądowego.

30. Określenie zakresu uprawnień dochodzeniowych, jak i koniecznych zabezpieczeń, pozostawiono przypuszczalnie w gestii prawa krajowego. Artykuł 10 ustęp 1 *de facto* pozostawia państwom członkowskim wiele opcji otwartych, określając, iż uprawnienia dochodzeniowe „mogą być wykonywane: a) bezpośrednio, b) we współpracy z innymi organami lub przedsiębiorstwami rynkowymi lub c) poprzez składanie wniosków do właściwych organów sądowych". Wydaje się, że pozwala to na rozbieżności w praktykach krajowych, np. w kwestii tego, czy i w jakich okolicznościach wymagany jest nakaz organu sądowego.

31. Choć niektóre systemy prawa krajowego mogą już zawierać odpowiednie zabezpieczenia proceduralne i zabezpieczenia z zakresu ochrony danych, jednak w celu zagwarantowania pewności prawa osobom, których dane dotyczą, należy wprowadzić pewne objaśnienia i określić pewne wymogi minimalne dotyczące zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych na poziomie unijnym, w ramach proponowanego rozporządzenia, jak zostanie to omówione poniżej.

32. EIOD podkreśla iż, co do zasady, w sytuacji, gdy prawodawstwo unijne zobowiązuje państwa członkowskie do zastosowania na poziomie krajowym środków, które mają wpływ na prawa podstawowe (takie jak prawo do prywatności i prawo do ochrony danych osobowych), prawodawstwo takie powinno również wymagać, aby jednocześnie ze środkami ograniczającymi stosowane były również skuteczne środki ochrony właściwych praw podstawowych. Innymi słowy, harmonizacji środków potencjalnie naruszających prywatność powinna towarzyszyć harmonizacja odpowiednich zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych, opartych na najlepszych praktykach.

33. Tego rodzaju podejście mogłoby ułatwić przeciwdziałanie zbyt daleko idącym rozbieżnościom na poziomie krajowym oraz zapewnienie wyższego i bardziej ujednoliconego poziomu ochrony danych osobowych w całej Unii Europejskiej.

34. Jeżeli harmonizacja minimalnych zabezpieczeń na obecnym etapie nie jest możliwa, EIOD zaleca, jako minimum, wprowadzenie do rozporządzenia szczególnego wymogu przyjęcia przez państwa członkowskie krajowych środków wykonawczych w celu zapewnienia koniecznych zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych. Jest to tym bardziej istotne, iż wybraną formą instrumentu prawnego jest rozporządzenie, które stosowane jest bezpośrednio, zatem zasadniczo nie musi oznaczać konieczności przyjęcia dalszych środków wykonawczych przez państwa członkowskie.

II.4. **Kontrole na miejscu (art. 10 ust. 2 lit. c))**

Odnośne przepisy

35. Wniosek wymaga, by przyznawane krajowym organom regulacyjnym uprawnienia dochodzeniowe obejmowały szczególne prawo do przeprowadzania kontroli na miejscu (art. 10 ust. 2 lit. c)).

Uwagi i zalecenia EIOD

36. Nie jest jasne, czy takie kontrole ograniczałyby się do majątku przedsiębiorstwa (lokali, gruntów i pojazdów) danego uczestnika rynku, czy mogłyby obejmować również majątek prywatny (lokale, grunty lub pojazdy) osób fizycznych. Równie niejasne jest, czy kontrole można przeprowadzać także bez uprzedzenia („naloty o świcie").

37. Jeżeli zamiarem Komisji jest zobowiązanie państw członkowskich do upoważnienia organu regulacyjnego do przeprowadzania kontroli na miejscu obejmujących majątek prywatny osób fizycznych lub na przeprowadzanie kontroli niezapowiedzianych, to, po pierwsze, należy wyraźnie to określić.

([1]) Należy zauważyć, że proponowane rozporządzenie nie przyznaje podobnych uprawnień dochodzeniowych ACER. Uprawnień takich nie przewidziano dla ACER również w rozporządzeniu (WE) nr 713/2009 Parlamentu Europejskiego i Rady z dnia 13 lipca 2009 r. ustanawiającym Agencję ds. Współpracy Organów Regulacji Energetyki, Dz.U. L 211 z 14.8.2009, s. 1.

38. Po drugie, EIOD podkreśla również, iż proporcjonalność kontroli na miejscu obejmujących majątek prywatny (np. prywatne mieszkania osób fizycznych) nie jest wcale kwestią oczywistą, zatem – jeśli jest przewidziana – wymaga szczególnego uzasadnienia.

39. Po trzecie, również w tym przypadku konieczne byłyby dodatkowe zabezpieczenia, w szczególności dotyczące warunków przeprowadzania takich kontroli. Na przykład, wniosek powinien między innymi określać, że kontrolę na miejscu można przeprowadzać w mieszkaniu osoby fizycznej wyłącznie w przypadku, gdy istnieje uzasadnione i konkretne podejrzenie, że w danym mieszkaniu są przechowywane dowody konieczne do wykazania poważnego naruszenia art. 3 i 4 rozporządzenia (tj. przepisów dotyczących zakazu wykorzystywania informacji wewnętrznych i manipulacji na rynku). Co istotne, wniosek powinien również wymagać nakazu sądowego we wszystkich państwach członkowskich ([1]).

40. Po czwarte, w celu zapewnienia proporcjonalności i zapobiegania nadmiernej ingerencji w życie prywatne, niezapowiedziane kontrole w mieszkaniach prywatnych powinny być objęte dodatkowym warunkiem, że w przypadku wizyty zapowiedzianej dowody mogłyby zostać zniszczone lub zmanipulowane. Warunek taki powinien zostać jednoznacznie określony w treści proponowanego rozporządzenia.

II.5. **Uprawnienia do żądania udostępnienia „istniejących rejestrów połączeń telefonicznych i przesyłu danych" (art. 10 ust. 2 lit. d))**

Odnośne przepisy

41. Artykuł 10 ustęp 2 litera d) wymaga, by uprawnienia krajowych organów regulacyjnych obejmowały również szczególne prawo do „żądania udostępnienia istniejących rejestrów połączeń telefonicznych i przesyłu danych".

Uwagi i zalecenia EIOD

42. EIOD docenia znaczenie rejestrów połączeń telefonicznych w przypadkach dotyczących wykorzystania informacji wewnętrznych, szczególnie dla ustalenia powiązań pomiędzy osobami posiadającymi informacje wewnętrzne a przedsiębiorstwami handlowymi. Zakres uprawnień, o których mowa, nie jest jednak wystarczająco jasno określony, a ponadto nie przewidziano również odpowiednich zabezpieczeń proceduralnych i zabezpieczeń z zakresu ochrony danych. W związku z tym EIOD zaleca doprecyzowanie rozporządzenia w sposób opisany poniżej. W szczególności uwzględnić należy następujące kwestie:

a) Jakiego rodzaju rejestry połączeń telefonicznych i przesyłu danych mogą być udostępniane na żądanie?

43. W celu zapewnienia pewności prawa wniosek powinien przede wszystkim wyjaśnić, jakiego rodzaju rejestry mogą być udostępniane w razie potrzeby na żądanie władz.

44. Wniosek powinien w szczególności ograniczać zakres uprawnień dochodzeniowych do (i) treści rejestrów połączeń telefonicznych, poczty elektronicznej i innych przesyłanych danych, które są już gromadzone – w sposób rutynowy i zgodny z prawem – przez przedsiębiorstwa dla potrzeb prowadzonej działalności gospodarczej w celu udokumentowania transakcji, oraz do (b) danych o ruchu (np. kto wykonał połączenie lub przesłał informację, do kogo i kiedy), które są już dostępne bezpośrednio u zainteresowanych uczestników rynku (przedsiębiorstw handlowych).

45. Ponadto rozporządzenie powinno określać, że rejestry muszą być gromadzone w celach legalnych i w zgodzie z obowiązującymi przepisami z zakresu ochrony danych, w tym zgodnie z wymogiem udzielania odpowiednich informacji osobom, których dane dotyczą, na mocy art. 10 i 11 dyrektywy 95/46/WE.

b) Co oznacza określenie „istniejące"?

46. EIOD z uznaniem przyjmuje fakt, że wniosek ogranicza omawiane prawo do „istniejących" rejestrów, a tym samym nie wymaga, by uprawnienia organów regulacyjnych obligowały przedsiębiorstwo handlowe lub osobę trzecią do celowego przechwytywania, monitorowania i rejestrowania połączeń telefonicznych lub przesyłu danych dla potrzeb dochodzenia.

47. W celu uniknięcia wszelkich wątpliwości zamierzenie to należy jednak doprecyzować – przynajmniej w jednym z motywów. Należy uniknąć sytuacji, w której pozostawia się pole do interpretacji proponowanego rozporządzenia jako podstawy prawnej, która sprawi, że krajowe organy regulacyjne będą mogły przechwytywać, monitorować lub rejestrować połączenia bądź transmisję danych, w sposób niejawny lub jawny, z nakazem lub bez niego.

c) Czy można żądać udostępnienia treści rozmów telefonicznych i przesyłu danych, czy jedynie danych o ruchu?

48. W tekście wniosku jest mowa o „istniejących rejestrach połączeń telefonicznych i przesyłu danych". Nie jest wystarczająco jasne, czy można żądać udostępnienia zarówno treści istniejących danych i łączności telefonicznej, jak i danych o ruchu (tj. kto wykonał połączenie lub przesłał informację, do kogo i kiedy).

49. Powyższą kwestię należy doprecyzować w przepisach proponowanego rozporządzenia. Jak wspomniano w pkt 43–45, należy jasno określić, jakiego rodzaju rejestry mogą być udostępniane na żądanie, a przede wszystkim należy zadbać o to, by rejestry takie były gromadzone zgodnie z obowiązującymi przepisami z zakresu ochrony danych.

d) Czy można żądać udostępnienia rejestrów przez dostawców usług internetowych i firmy telekomunikacyjne?

50. Wniosek powinien określać w sposób jednoznaczny, od kogo krajowe organy regulacyjne mogą żądać udostępnienia rejestrów. W tej kwestii EIOD zakłada, że art. 10

([1]) Zob. np. wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Funke* przeciwko *Francji* (sprawa nr 82/1991/334/407) z dnia 25 lutego 1993 r., pkt 55–57.

ust. 2 lit. d) w zamierzeniu nie powinien zezwalać organom krajowym na żądanie udostępnienia danych o ruchu przez dostawców „publicznie dostępnych usług łączności elektronicznej" [1] (takich jak operatorzy telefoniczni lub dostawcy usług internetowych).

51. Wniosek *de facto* nie dotyczy wszystkich takich dostawców, a ponadto nie posługuje się określeniem „dane o ruchu". Co istotne, nie odnosi się on, ani w sposób domyślny, ani wyraźny, do postanowienia mówiącego o tym, że należałoby zastosować odstępstwo od wymogów dyrektywy o prywatności i łączności elektronicznej [2], która określa ogólną zasadę, iż dane o ruchu mogą być poddawane dalszemu przetwarzaniu wyłącznie do celów naliczania opłat abonenta i opłat rozliczeń międzyoperatorskich.

52. W celu uniknięcia wszelkich wątpliwości EIOD zaleca, by fakt, iż wniosek nie stanowi podstawy prawnej, na podstawie której można żądać udostępnienia danych przez dostawców publicznie dostępnych usług łączności elektronicznej, został wyraźnie uwzględniony w tekście proponowanego rozporządzenia – przynajmniej w jednym z motywów.

e) Czy można żądać udostępnienia rejestrów przez inne osoby trzecie?

53. Ponadto, wniosek powinien wyjaśniać, czy krajowe organy regulacyjne mogą żądać udostępnienia rejestrów wyłącznie przez uczestników rynku objętych dochodzeniem, czy są również uprawnione do tego, by żądać od osób trzecich udostępnienia ich rejestrów (np. od strony w transakcji z uczestnikiem rynku objętym dochodzeniem lub od hotelu, w którym przebywała osoba podejrzana o wykorzystanie informacji wewnętrznych).

f) Czy można żądać udostępnienia rejestrów prywatnych?

54. Wreszcie, wniosek powinien także wyjaśniać, czy organy mogą również żądać udostępnienia rejestrów prywatnych osób fizycznych, takich jak pracownicy lub członkowie kadry zarządzającej uczestnika rynku objętego dochodzeniem (np. wiadomości SMS przesyłanych z osobistych urządzeń przenośnych lub historii wyszukiwania domowego łącza internetowego przechowywanej na domowym komputerze).

55. Proporcjonalność żądania udostępnienia rejestrów prywatnych jest dyskusyjna, i – jeśli jest przewidziana – powinna być szczególnie uzasadniona.

56. Podobnie jak w przypadku kontroli na miejscu (zob. pkt 35–40 powyżej), wniosek powinien wymagać nakazu wystawionego przez organ sądowy, a także dalszych szczególnych zabezpieczeń w przypadku, gdy organy żądają udostępnienia jakichkolwiek rejestrów prywatnych.

II.6. **Zgłaszanie podejrzenia nadużycia na rynku (art. 11): celowość i zatrzymywanie danych**

Odnośne przepisy

57. W związku ze współpracą transgraniczną ACER przypada istotna rola ostrzegania krajowych organów regulacyjnych o potencjalnych nadużyciach na rynku i ułatwiania wymiany informacji. W celu ułatwienia współpracy art. 11 ust. 2 zawiera również szczególny wymóg, aby krajowe organy regulacyjne informowały ACER „w możliwie szczegółowy sposób" w przypadku, gdy mają uzasadnione podstawy, aby podejrzewać naruszenie proponowanego rozporządzenia. W celu zapewnienia skoordynowanego podejścia art. 11 ust. 3 wymaga również wymiany informacji pomiędzy krajowymi organami regulacyjnymi, właściwymi organami finansowymi, ACER oraz Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych („ESMA") [3].

Uwagi i zalecenia EIOD

58. Zgodnie z zasadą celowości [4], wniosek powinien określać wyraźnie, iż wszelkie dane osobowe przekazywane na podstawie art. 11 proponowanego rozporządzenia (zgłoszenia dotyczące podejrzenia nadużycia na rynku) powinny być wykorzystywane wyłącznie w celu zbadania danego zgłoszonego podejrzenia nadużycia na rynku. Informacje takie w żadnym wypadku nie powinny być wykorzystywane dla potrzeb niezgodnych z takim celem.

59. Dane nie powinny być również zatrzymywane przez długi czas. Jest to jeszcze bardziej istotne w przypadkach, gdzie można wykazać, iż pierwotne podejrzenie było nieuzasadnione. W takich przypadkach dalsze zatrzymywanie danych wymaga szczególnego uzasadnienia [5].

60. W tej kwestii wniosek powinien w pierwszej kolejności określić maksymalną długość okresu zatrzymania, przez który ACER i inni odbiorcy informacji mogą przechowywać dane, przy uwzględnieniu celu takiego przechowywania danych. O ile w efekcie podejrzenia nadużycia na rynku nie wszczęto szczegółowego dochodzenia, które nadal znajduje się w toku, po upływie takiego okresu wszelkie dane osobowe związane ze zgłoszonym podejrzeniem nadużycia na rynku powinny zostać usunięte

[1] Zob. art. 2 lit. c) dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej), Dz.U. L 108 z 24.4.2002, s. 33.

[2] Zob. art. 6 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37.

[3] ESMA jest niezależnym organem unijnym, który przyczynia się do zabezpieczenia stabilności systemu finansowego Unii Europejskiej poprzez zapewnianie integralności, przejrzystości, efektywności i prawidłowego funkcjonowania rynków papierów wartościowych oraz lepszej ochrony inwestorów.

[4] Zob. art. 6 ust. 1 lit. b) dyrektywy 95/46/WE i art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 45/2001.

[5] Dla przykładu, EIOD odwołuje się w tym kontekście do orzeczenia Europejskiego Trybunału Praw Człowieka w sprawie *S i Marper* przeciwko *Zjednoczonemu Królestwu (2008)* (4 grudnia 2008 r.) (skargi nr 30562/04 i 30566/04), zgodnie z którym długoterminowe zatrzymywanie danych osób nieskazanych za przestępstwo było naruszeniem ich prawa do prywatności wynikającego z art. 8 Konwencji o ochronie praw człowieka.

z rejestrów wszystkich odbiorców. O ile z oczywistych względów nie jest wskazany dłuższy okres zatrzymania, w opinii EIOD usunięcie danych powinno nastąpić nie później niż dwa lata po dacie zgłoszenia danego podejrzenia ([1]).

61. W przypadku, gdy podejrzenie okazuje się nieuzasadnione lub dochodzenie zostaje zamknięte bez podjęcia dalszych działań, wniosek powinien zobowiązywać zgłaszający je organ regulacyjny, ACER oraz każdą osobę trzecią posiadającą dostęp do informacji dotyczących danego podejrzenia nadużycia na rynku do niezwłocznego poinformowania tych podmiotów, tak, by były one w stanie odpowiednio zaktualizować własne rejestry (lub usunąć ze swoich rejestrów informacje dotyczące zgłoszonego podejrzenia, odpowiednio, ze skutkiem natychmiastowym bądź po upływie proporcjonalnego okresu zatrzymania) ([2]).

62. Powyższe przepisy powinny pomóc w doprowadzeniu do sytuacji, w której – w przypadku, gdy dane podejrzenie nie znajduje potwierdzenia (lub wręcz nie podjęto w jego sprawie dochodzenia) lub gdy z ustaleń wynika, że podejrzenie jest nieuzasadnione – niewinne osoby nie będą pozostawały na „czarnej liście" i „w kręgu podejrzeń" przez nadmiernie długi okres (zob. art. 6 lit. e) dyrektywy 95/46/WE i odpowiadający mu art. 4 lit. e) rozporządzenia (WE) nr 45/2001).

II.7. **Przekazywanie danych do państw trzecich (art. 14)**

Odnośne przepisy

63. Artykuły 7, 8 i 11 proponowanego rozporządzenia przewidują wymianę danych i informacji pomiędzy ACER, ESMA i organami państw członkowskich. Artykuł 14 („Stosunki z państwami trzecimi") przewiduje, że ACER „może zawierać porozumienia administracyjne z organizacjami międzynarodowymi oraz z administracjami państw trzecich." Może to prowadzić do przekazywania danych osobowych przez ACER – i ewentualnie przez ESMA lub organy państw członkowskich – organizacjom międzynarodowym i organom państw trzecich.

Uwagi i zalecenia EIOD

64. EIOD zaleca, by w art. 14 wniosku doprecyzowano, iż przekazywanie danych osobowych może odbywać się wyłącznie w zgodzie z art. 9 rozporządzenia (WE) nr 45/2001 oraz art. 25 i 26 dyrektywy 95/46/WE. W szczególności, przekazywanie danych w relacji międzynarodowej powinno odbywać się tylko wówczas, gdy dane państwo trzecie zapewnia odpowiedni poziom ochrony danych lub, w przypadku osób prawnych lub fizycznych niezapewniających odpowiedniej ochrony, gdy administrator danych powołuje się na stosowne zabezpieczenia dotyczące ochrony prywatności, praw podstawowych oraz wolności osób fizycznych i związane z wykonaniem odpowiednich praw.

65. EIOD podkreśla, że stosowanie odstępstw (takich jak wymienione w art. 9 ust. 6 rozporządzenia (WE) nr 45/2001 i w art. 26 ust. 1 dyrektywy) zasadniczo nie powinno służyć uzasadnieniu masowego, systematycznego lub strukturalnego przekazywania danych do państw trzecich.

II.8. **Uprzednie sprawdzanie działań koordynacyjnych ACER w związku z dochodzeniami**

66. Niektóre dane wymieniane pomiędzy ACER, ESMA i różnymi organami państw członkowskich w związku z podejrzeniami naruszenia przepisów mogą zawierać dane osobowe, takie jak tożsamość domniemanych sprawców i innych zaangażowanych osób (np. świadków, osób zgłaszających przypadki naruszenia, pracowników lub innych osób występujących w imieniu przedsiębiorstw uczestniczących w transakcji).

67. Artykuł 27 ustęp 1 rozporządzenia (WE) nr 45/2001 stanowi, iż „operacje przetwarzania mogące ze swej natury, przez swój zakres lub swoje cele stworzyć konkretne zagrożenia dla praw i wolności podmiotów danych, podlegają uprzedniemu sprawdzeniu przez europejskiego inspektora ochrony danych". Artykuł 27 ustęp 2 precyzuje, że „przetwarzanie danych" dotyczących „podejrzeń o popełnienie przestępstwa" i „przestępstw" tworzy takie zagrożenia, i wymaga uprzedniego sprawdzenia. Ze względu na rolę przewidzianą dla ACER w ramach koordynowania dochodzeń wydaje się prawdopodobne, że będzie ona przetwarzać dane dotyczące „podejrzeń o popełnienie przestępstwa", a tym samym jej działania będą podlegać uprzedniemu sprawdzeniu ([3]).

68. W ramach procedury uprzedniego sprawdzania EIOD może udzielać ACER dalszych wskazówek i szczegółowych zaleceń dotyczących zgodności z przepisami dotyczącymi ochrony danych. Uprzednie sprawdzanie działań ACER może być również źródłem wartości dodanej, ze względu na fakt, że rozporządzenie (WE) nr 713/2009 ustanawiające ACER nie zawiera żadnego odniesienia do kwestii ochrony danych osobowych, i nie było przedmiotem opinii legislacyjnej EIOD.

III. **WNIOSKI**

69. Wniosek powinien doprecyzować, czy w kontekście monitorowania rynku i przekazywania danych mogą być przetwarzane dane osobowe, a także jakie zabezpieczenia mają zastosowanie. Jeżeli natomiast nie przewiduje się przetwarzania danych osobowych (lub takie przetwarzanie miałoby wyłącznie charakter wyjątkowy i ograniczałoby się do rzadkich przypadków, gdy przedsiębiorca zajmujący się hurtową sprzedażą energii nie jest osobą prawną, lecz osobą fizyczną), należy to jednoznacznie określić w rozporządzeniu – przynajmniej w jednym z motywów.

([1]) W przypadkach, gdy podejrzenie okazuje się uzasadnione i powoduje przeprowadzenie dochodzenia, wniosek powinien określać konkretny – nienadmierny – okres zatrzymania danych po zakończeniu dochodzenia.

([2]) Informacje takie należy również udostępnić osobie, której dane dotyczą.

([3]) Należy podkreślić, że przetwarzanie danych przez organy krajowe może również podlegać uprzedniemu sprawdzeniu przez krajowe lub regionalne organy ds. ochrony danych na podstawie krajowych przepisów z zakresu ochrony danych przyjętych na mocy art. 20 dyrektywy 95/46/WE.

70. Należy doprecyzować i wzmocnić przepisy dotyczące ochrony danych, bezpieczeństwa danych i rozliczalności, zwłaszcza jeśli przetwarzanie danych osobowych miałoby odgrywać bardziej zasadniczą rolę. Komisja powinna zadbać o stosowne mechanizmy kontroli w celu zapewnienia zgodności z zasadami ochrony danych i dowodów takiej zgodności („rozliczalność").

71. Wniosek powinien doprecyzować, czy kontrole na miejscu byłyby ograniczone do majątku przedsiębiorstwa (lokale i pojazdy) danego uczestnika rynku, czy obejmowałyby również majątek prywatny (lokale lub pojazdy) osób fizycznych. W tym ostatnim przypadku należałoby jednoznacznie uzasadnić konieczność i proporcjonalność takiego prawa oraz wprowadzić wymóg nakazu sądowego i dodatkowych zabezpieczeń. Kwestie te powinny być określone w proponowanym rozporządzeniu w sposób jednoznaczny.

72. Należy doprecyzować zakres uprawnień do żądania udostępnienia „istniejących rejestrów połączeń telefonicznych i przesyłu danych". Wniosek powinien określać w sposób jednoznaczny, jakie rejestry mogą być udostępniane na żądanie, i przez kogo. Fakt, że nie można żądać udostępnienia danych przez dostawców publicznie dostępnych usług łączności elektronicznej, powinien być wyraźnie wzmiankowany w tekście proponowanego rozporządzenia – przynajmniej w jednym z motywów. Wniosek powinien również doprecyzować, czy organy mogą żądać udostępnienia również prywatnych rejestrów osób fizycznych, np. pracowników lub członków kadry zarządzającej uczestnika rynku objętego dochodzeniem (np. wiadomości SMS wysyłanych z osobistych urządzeń przenośnych lub historii wyszukiwania domowego łącza internetowego). W takim przypadku należałoby jednoznacznie uzasadnić konieczność i proporcjonalność takiego prawa, a wniosek powinien również określać wymóg nakazu wystawionego przez organ sądowy.

73. W kwestii zgłaszania podejrzeń nadużycia na rynku wniosek powinien wyraźnie określać, że wszelkie dane osobowe zawarte w takich zgłoszeniach powinny być wykorzystywane wyłącznie do celów dochodzenia w sprawie danego zgłoszonego podejrzenia nadużycia na rynku. O ile w efekcie podejrzenia nadużycia na rynku nie wszczęto szczegółowego dochodzenia, które nadal znajduje się w toku (lub o ile podejrzenie nie okazało się uzasadnione, w efekcie czego przeprowadzono dochodzenie), po upływie wyznaczonego okresu wszelkie dane osobowe związane ze zgłoszonym podejrzeniem nadużycia na rynku powinny zostać usunięte z rejestrów wszystkich odbiorców (o ile nie występują inne przesłanki, nie później niż dwa lata od daty zgłoszenia). Ponadto w przypadku, gdy dane podejrzenie okazuje się nieuzasadnione lub dochodzenie zostaje zamknięte bez podjęcia dalszych działań, strony uczestniczące w wymianie informacji powinny również przesyłać sobie wzajemnie aktualne informacje.

74. W kwestii przekazywania danych osobowych do państw trzecich wniosek powinien doprecyzować, że przekazywanie danych osobom prywatnym lub fizycznym w kraju trzecim, który nie zapewnia odpowiedniej ochrony, możliwe jest zasadniczo wyłącznie w przypadku, gdy administrator danych powołuje się na stosowne zabezpieczenia dotyczące ochrony prywatności, praw podstawowych oraz wolności osób fizycznych i związane z wykonaniem odpowiednich praw.

75. ACER powinna wystąpić do EIOD o uprzednie sprawdzenie jej działań z zakresu przetwarzania danych osobowych w związku z koordynacją dochodzeń na podstawie art. 11 proponowanego rozporządzenia.

Sporządzono w Brukseli dnia 21 czerwca 2011 r.

Giovanni BUTTARELLI

Zastępca Europejskiego Inspektora Ochrony Danych